Security Target

BlackBerry® Device Software 5.0.0

Document Version 5.0

BlackBerry Certifications

Research In Motion

Document and Contact Information

Version	Date	Description
5.0	March 4, 2010	Final Revision

Contact	Corporate Office
BlackBerry Certifications certifications@rim.com (519) 888-7465 ext. 72921	**Research In Motion** 295 Phillip Street Waterloo, Ontario Canada N2L 3W8 www.rim.com www.blackberry.com

Contents

1 ST Introduction 1
1.1 ST Reference 1
1.2 TOE Reference 1
1.3 Evaluated Configuration 1
1.4 TOE Overview 1
1.5 TOE Type 2
1.6 TOE Description 3
2 Conformance Claim 10
3 Security Problem Definition 11
3.1 Threats 11
3.2 Organisational Security Policies 11
3.3 Assumptions 11
4 Security Objectives 13
4.1 TOE Security Objectives 13
4.2 Environmental Security Objectives 13
4.3 Security Objectives Rationale 14
5 Extended Components Definition 16
5.1 FCS_VAL_EXP.1 Cryptographic Module Validation 16
5.2 FDP_SDP_EXP.1 Stored Data Non-Disclosure 16
5.3 FDP_SDP_EXP.2 Stored Data Deletion 16
5.4 FTA_SSL_EXP.4 Event-Initiated Session Locking 16
6 Security Requirements 17
6.1 Conventions 17
6.2 Security Functional Requirements 17
6.3 Security Assurance Requirements 38
6.4 Security Requirements Rationale 39
7 TOE Summary Specification 50
7.1 Security Functions 50
7.2 Assurance Measures 58
7.3 TOE Security Specification 58
8 Baseline Configuration 69

8.1 Baseline IT Policy Configuration 69
8.2 Baseline Software Configuration 70
8.3 Baseline User Guidance 71
9 Glossary 72

List of Tables

Table 1. User Data Protected by Content Protection Feature 5
Table 2. Mapping of Security Objectives 14
Table 3. TOE Assurance Components 39
Table 4. Mapping of SFRs to Security Objectives 40
Table 5. SFR Dependencies 43
Table 6. SAR Dependencies 48
Table 7. IT Commands 52
Table 8. IT Policy Rules 52
Table 9. Software Configuration Rules 56
Table 10. Mapping of TOE Security Functions to SFRs 59
Table 11. Mapping of TOE Assurance Measures to SARs 65
Table 12. Baseline IT Policy Configuration 69
Table 13. Baseline Software Configuration 70

List of Figures

Figure 1. BlackBerry Solution Architecture 2
Figure 2. BlackBerry Device Hardware Block Diagram 8
Figure 3. TOE Physical Boundary 9

1 ST Introduction

1.1 ST Reference

The following information identifies this document:

Title: Security Target: BlackBerry® Device Software 5.0.0

Version: 5.0

1.2 TOE Reference

The following information identifies the TOE:

Title: BlackBerry® Device Software 5.0.0

Version: 5.0

1.3 Evaluated Configuration

Evaluated Configuration consists of the following;

- BlackBerry 9700 series
- BlackBerry 9500 series

- 9700 Series BlackBerry® Device Software 5.0.0 (5.0.0.321 bundle 499, 5.0.0.344 bundle 541, 5.0.0.351 bundle 554)
    - Guidance documents for the BlackBerry 9700 series Handheld device can be found on the BlackBerry.com website at; http://docs.blackberry.com/en/smartphone_users/subcategories/?userType=1&category=BlackBerry+Smartphones&subCategory=BlackBerry+Bold+9700+Series

- 9500 Series BlackBerry® Device Software 5.0.0 (5.0.0.320 bundle 497)
    - Guidance documents for the BlackBerry 9500 series Handheld device are available on the BlackBerry.com website at; http://docs.blackberry.com/en/smartphone_users/subcategories/?userType=1&category=BlackBerry+Smartphones&subCategory=BlackBerry+Storm2+9500+Series

Visit http://www.blackberry.com for up to date device availability information.

The evaluated configurations consist of the following:

Software version numbers are displayed on a BlackBerry device by navigating to the Options list and selecting the About item.

1.4 TOE Overview

BlackBerry® is the leading wireless solution that allows users to stay connected to a full suite of applications, including email, phone, enterprise applications, Internet, Short Messaging Service (SMS), and organiser information. BlackBerry is a totally integrated package that includes innovative software, advanced BlackBerry devices and wireless network service, providing a seamless solution. The BlackBerry architecture is shown in the following figure.

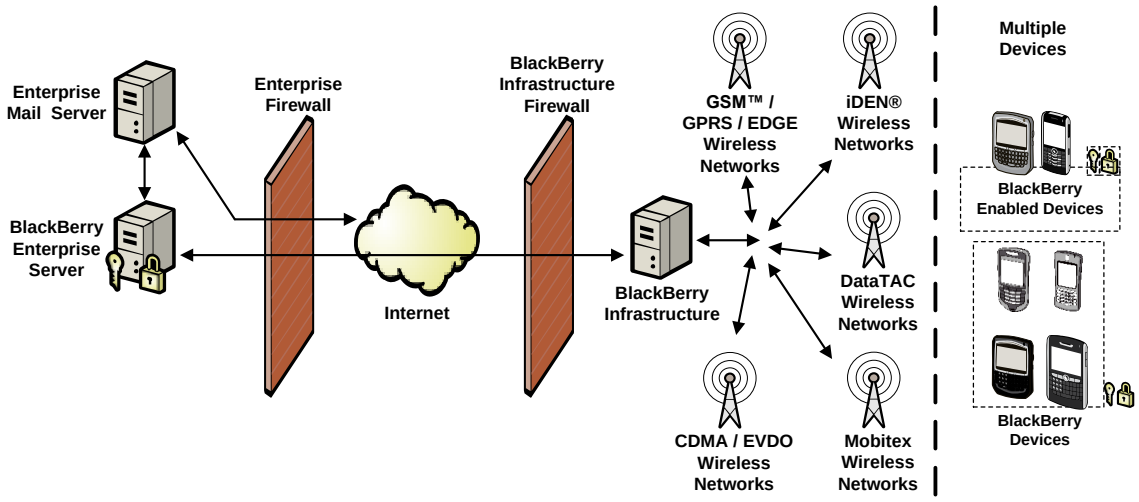

Figure 1. BlackBerry Solution Architecture

BlackBerry Enterprise Server software tightly integrates with Microsoft® Exchange, IBM® Lotus® Domino®, and Novell® GroupWise® (with the exclusion of Secure/Multipurpose Internet Mail Extensions (S/MIME) for Groupwise) while working with other existing enterprise systems to enable push-based access of wireless email and data. It allows users to securely send and receive email and information from enterprise data stores and applications. BlackBerry Enterprise Server provides simplified management and centralised control of the wireless environment with industry-standard performance monitoring capabilities, administrative tools, and wirelessly-enabled IT policies. BlackBerry Enterprise Server also enables several other productivity enhancements, including attachment viewing for popular file formats, wireless calendar synchronisation, and remote address lookup, and allows IT departments to benefit from a scalable and flexible solution that meets their evolving wireless requirements.

BlackBerry devices are built on industry-leading wireless technology, allowing users to receive email and information automatically with no need to request for delivery. Additionally, users are notified when new information arrives, making it easier to stay informed.

BlackBerry devices also provide an intuitive user experience. Users simply click on an email address, telephone number, or URL inside a message to automatically begin composing the new email, make the call, or link to the web page. BlackBerry device users can also easily navigate through icons, menus, and options with the roll-and-click trackwheel and quickly compose messages or enter data using the device keyboard.

BlackBerry provides advanced security features to meet the strict confidentiality and security requirements of the public sector. Data remains encrypted at all points between the device and BlackBerry Enterprise Server using FIPS 140-2 validated cryptography, allowing users to feel confident about wirelessly sending and receiving sensitive information.

BlackBerry operates on multiple high speed wireless networks. With wireless service available in North America, South America, Europe, Asia, Australia, and Africa, the BlackBerry solution can support enterprises around the world while providing options for wireless network and service choice.

Visit http://www.blackberry.com for more information on the BlackBerry solution.

1.5 TOE Type

Mobile Productivity Devices and Systems

1.6 TOE Description

1.6.1 TOE Features

1.6.1.1 Messaging

The BlackBerry solution provides a secure wireless extension of the enterprise messaging environment.

1.6.1.1.1 Email

The TOE integrates seamlessly with an existing email account, allowing the user to wirelessly send and receive email. Email is pushed to the TOE automatically, so the user can wirelessly receive email with the same speed and at least as much reliability as that of their desktop email program.

When the user moves or deletes email messages using the TOE, or marks messages read or unread, the changes are reconciled wirelessly between the device and the enterprise email account.

Wireless email messaging and reconciliation is mediated by the BlackBerry Enterprise Server.

1.6.1.1.2 PIM Data

The user can synchronise personal information management (PIM) items such as calendar entries, tasks, memos, and contacts wirelessly so that the entries on the TOE and the enterprise email account are consistent. If wireless PIM synchronisation is enabled, PIM items are synchronised over the wireless network automatically. With wireless PIM synchronisation and wireless email reconciliation, the user does not need to physically connect the TOE to their desktop to synchronise and reconcile messaging and PIM data.

The user can create or edit meeting requests and accept or decline invitations using the TOE. Any changes are synchronised wirelessly between the TOE and the enterprise email account.

When wireless PIM synchronisation is enabled, an initial data synchronisation between the TOE and the enterprise mail server to fully synchronise both sides is performed in a way that avoids data loss on either side and is optimised for wireless transmission. After the initial synchronisation is complete, incremental changes are synchronised bi-directionally between the TOE and the enterprise mail server.

PIM data synchronisation is mediated by the BlackBerry Enterprise Server.

1.6.1.1.3 Attachments

The BlackBerry Enterprise Server enables the user to use the TOE to view supported email attachments in a format that retains the original layout, appearance, and navigation of the attachment. The device attachment viewer is fully integrated with the device mail application and the BlackBerry Enterprise Server.

Because the BlackBerry Enterprise Server interprets and converts email attachments in binary format, the applications that are associated with the attachment format are not required to be installed on the BlackBerry Enterprise Server, and there is no risk of infection on the device by macro viruses that operate within those applications.

The attachment viewer is installed automatically with the BlackBerry Enterprise Server software and supports many formats, such as .doc, .dot, .xls, .ppt, .pdf, .txt, .html, .htm, .wpd, and .zip document formats and .jpg, .bmp, .gif, .png, and .tif graphic formats.

1.6.1.1.4 Remote Address Lookup

Remote address lookup enables the user to search for a recipient in their enterprise directory when they compose an email message using the TOE.

The user can search using letters from the entry's first name, last name, or both. The BlackBerry Enterprise Server searches the enterprise directory and returns (up to) the 20 closest matches. If the desired name does not appear in the list, the user can request the next 20 search results. When the user selects a match, the entry can be added to the personal address book.

1.6.1.2 S/MIME Support Package

The S/MIME Support Package for BlackBerry devices is designed to enable BlackBerry device users who are already sending and receiving S/MIME messages using their computer email application to send and receive S/MIME-protected messages using their BlackBerry devices. The S/MIME Support Package for BlackBerry devices is designed to work with S/MIME email clients including Microsoft Outlook® and Microsoft Outlook Express, and with popular PKI components, including Netscape®, Entrust® Authority™ Security Manager version 5 and later, and Microsoft certificate authorities.

The S/MIME Support Package for BlackBerry devices includes tools for obtaining certificates and transferring them to the BlackBerry device. This means that BlackBerry devices with the S/MIME Support Package for BlackBerry devices installed can decrypt messages that are encrypted using S/MIME encryption and BlackBerry device users can read the decrypted messages on their BlackBerry devices, and that BlackBerry device users can sign, encrypt, and send S/MIME messages from their BlackBerry devices. Without the S/MIME Support Package for BlackBerry devices the BlackBerry Enterprise Server sends a message to the BlackBerry device in which the message body includes a statement that the S/MIME message cannot be decrypted.

In order to use the S/MIME functionality the BES must be configured to allow S/MIME and an activation cod from http://www.blackberry.com/updates must be installed.

The S/MIME Support Package for BlackBerry devices includes support for the following features:

- Certificate and private key synchronization and management using the Certificate Synchronization Manager included in the BlackBerry Desktop Software
- Encrypting and decrypting messages, including PIN messages, verifying digital signatures, and digitally signing outgoing messages
- Searching for and retrieving certificates and certificate status over the wireless network using PKI protocols
- Smart cards on BlackBerry devices

1.6.1.3 BlackBerry Mobile Data Service

The BlackBerry Enterprise Server provides the BlackBerry Browser and third-party Java™ applications with secure access to the Internet and online enterprise data and applications. The BlackBerry Enterprise Server can provide a link to standard servers on the enterprise intranet or Internet using standard Internet protocol, such as HTTP, and encrypts content in transit using the same encryption standard used to encrypt email and other BlackBerry data.

1.6.1.4 IT Policy

1.6.1.4.5 Wireless IT Policy

Wireless IT policy enables the BlackBerry Enterprise Server administrator to define settings and push them wirelessly to the TOE for enforcement. A policy consists of rules that define the security, PIM synchronisation settings, and other behaviours of the TOE. Because the policy is pushed wirelessly, it is effective immediately.

1.6.1.4.6 Wireless IT Commands

The BlackBerry Enterprise Server administrator can wirelessly and securely send commands to the TOE for execution. Wireless IT commands include **Erase Data and Disable Handheld** and **Set Password and Lock Handheld**.

1.6.1.5 Security

1.6.1.5.7 BlackBerry Infrastructure

Communication between the TOE and a BlackBerry Enterprise Server or another BlackBerry device is routed by the BlackBerry Infrastructure, the link between the wired and wireless networks in the BlackBerry solution. The communication between the TOE and the BlackBerry Infrastructure utilises the RIM-proprietary Gateway Message Envelope (GME) protocol.

1.6.1.5.8 Secure Communication

The BlackBerry solution enables users to send and receive email and access enterprise data wirelessly, while seamlessly protecting data against attack. Data is encrypted while in transit between the TOE and a BlackBerry Enterprise Server or another BlackBerry device and is never decrypted between these two endpoints.

1.6.1.5.9 Third Party Application Control

The BlackBerry Enterprise Server administrator can control third-party Java applications on the TOE in the following ways:

- Allow or disallow third-party applications from being downloaded to the TOE
- Configure policies that define the type of connections that third-party applications can establish (for example, opening network connections inside the enterprise firewall)
- Allow or prevent the installation of specific third-party applications on the TOE
- Limit the permissions of third-party applications, including the resources that the application can access and the types of connections that it can establish

1.6.1.5.10 Content Protection

The content protection feature encrypts data that is stored on the TOE using Advanced Encryption Standard with 256 bit encryption (AES-256). The TOE also encrypts email messages and meeting requests that it receives when it is locked. If the content protection feature is enabled, the data identified in the following table is protected.

Table 1. User Data Protected by Content Protection Feature

Application	User Data
Email	Subject, email addresses, message body, attachments
Calendar	Subject, location, organiser, attendees, notes included in the appointment or meeting request
Memo Pad	Title, information in the note body
Tasks	Subject, information in the task body
Contacts	All information except for title and category
Auto Text	All entries that the original text is replaced with
BlackBerry Browser	Pushed content, saved web sites, browser cache

1.6.1.5.11 Protected storage of external memory on a BlackBerry device

The BlackBerry device is designed to encrypt multimedia data stored on an external memory device according to the External File System Encryption Level IT policy rule or the corresponding BlackBerry device setting.

The BlackBerry device is designed to support:

- File encryption by encrypting specific files on the external memory device using AES-256
- Access control to objects on the external memory device using code signing

The external memory device stores the media card master keys that the BlackBerry device is designed to use to decrypt and encrypt files on the external memory device. The BlackBerry device is designed to use either a device key stored in the Non-Volatile (NV) store in the BlackBerry device Random Access Memory (RAM) or a user-provided password to encrypt the master keys.

The BlackBerry device is designed to permit code signing keys in the header information of the encrypted file on the external memory device. The BlackBerry device is designed to check the code signing keys when the BlackBerry device opens the input or output streams of the encrypted file.

The BlackBerry device, any computer platform, and other devices that use the external memory device can modify encrypted files (for example, truncate files) on the external memory device. The BlackBerry device is not designed to perform integrity checks on the encrypted file data.

1.6.2 TOE Security Function Policies

The TOE enforces access and flow control security functional policies (SFPs) that control access to TOE functionality and resources.

1.6.2.1 IT Policy SFP

The IT policy security function policy (ITPolicy_SFP) controls the application of an IT policy configuration received from a BlackBerry Enterprise Server. The IT policy configuration is only applied if the TOE determines the configuration was sent by an authorised BlackBerry Enterprise Server.

1.6.2.2 Local Administration SFP

The local administration SFP (LocalAdmin_SFP) controls the ability of the TOE user to manage the TSF through the local administration screens. The TOE user can modify a particular configuration item only if permitted by the IT policy configuration. The TOE user is explicitly denied the ability to modify the IT policy configuration of the TOE.

1.6.2.3 GME SFP

The GME SFP (GME_SFP) controls the information flow between the TOE and a BlackBerry Enterprise Server, and PIN messaging between the TOE and another BlackBerry device.

1.6.2.4 IT Command SFP

The IT command SFP (ITCommand_SFP) controls the execution of a wireless IT command received from a BlackBerry Enterprise Server. The IT command is only executed if the TOE determines the command was sent by an authorised BlackBerry Enterprise Server.

1.6.2.5 PIM SFP

The PIM SFP (PIM_SFP) controls the wireless synchronisation of PIM data between the TOE and the corresponding enterprise email account.

1.6.2.6 Application Download SFP

The application download SFP (ApplicationDownload_SFP) controls the downloading and installation of third-party applications.

1.6.2.7 Application Flow SFP

The application flow SFP (ApplicationFlow_SFP) controls the communication initiated by a third-party application with an entity external to the TOE.

1.6.2.8 Cellular SFP

The cellular SFP (Cellular_SFP) controls the ability to send and receive cellular phone communication as well as SMS and Multimedia Messaging Service (MMS) messaging.

1.6.2.9 Radio SFP

The Radio SFP (Radio_SFP) controls the ability to send and receive Bluetooth, WiFi and Global Positioning System (GPS) communications.

1.6.2.10 Software Configuration SFP

The software configuration SFP (SWConfiguraion_SFP) allows or prevents the installation of specific third-party applications on the TOE and limits the permissions of third-party applications, including the resources that the application can access and the types of connections that it can establish.

1.6.2.11 Multimedia SFP

The multimedia SFP (Multimedia_SFP) controls the ability to take pictures, record video and voice notes, and store multimedia user data on the external memory device.

1.6.2.12 S/MIME SFP

The S/MIME SFP (S/MIME_SFP) controls the ability to send and receive S/MIME messages.

1.6.3 TOE Boundary

1.6.3.1 Physical Boundary

The TOE can be executed on all Java-based BlackBerry devices with at least 64 MB of memory. All BlackBerry devices share a set of core components, while several components are dependent on the device model. A block diagram of BlackBerry device hardware is shown in the following figure for reference purposes.

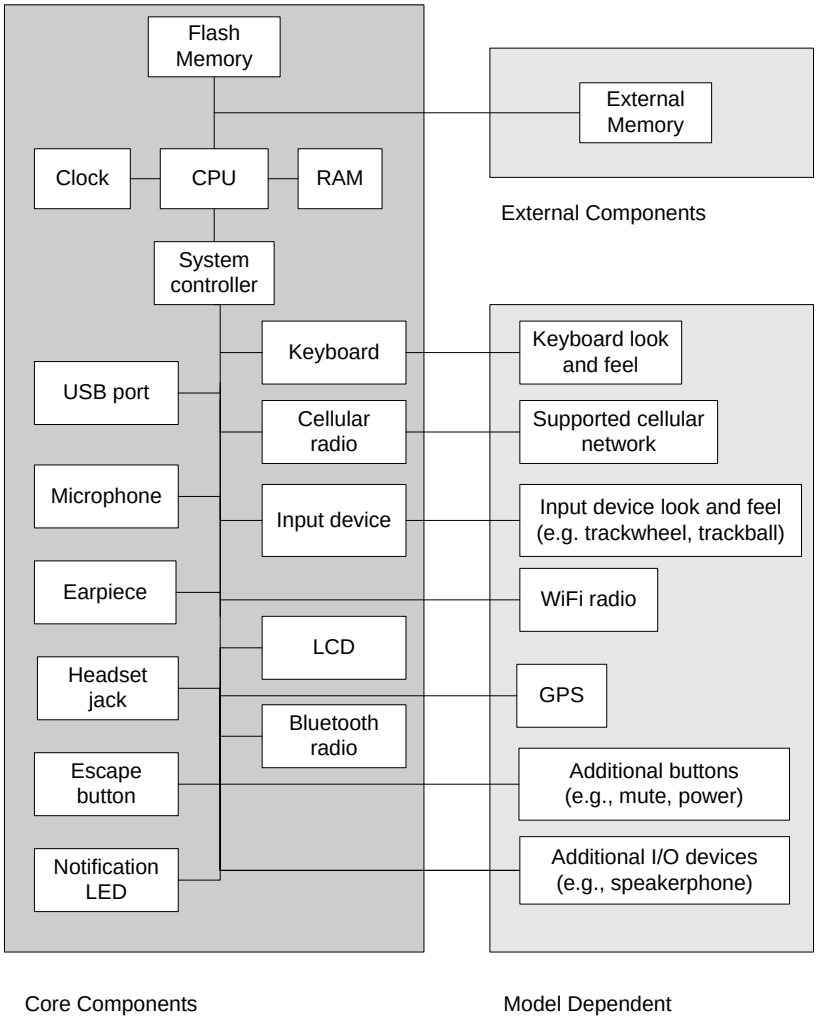

Figure 2. BlackBerry Device Hardware Block Diagram

The TOE includes a rich suite of applications and provides an application programming interface (API) to allow for third-party development of additional applications. The API consists of a Java Platform Micro Edition runtime environment, based on the CLDC 1.1 and MIDP 2.0 specifications, and BlackBerry API extensions that provide additional capabilities and tighter integration with BlackBerry devices. Supporting the API is the BlackBerry Platform, which is comprised of the BlackBerry Java Virtual Machine and the BlackBerry operating system. The TOE is defined as a software TOE that includes the BlackBerry Platform and the API that it supports but excludes the BlackBerry device hardware. The physical boundary of the TOE is shown in the following figure.

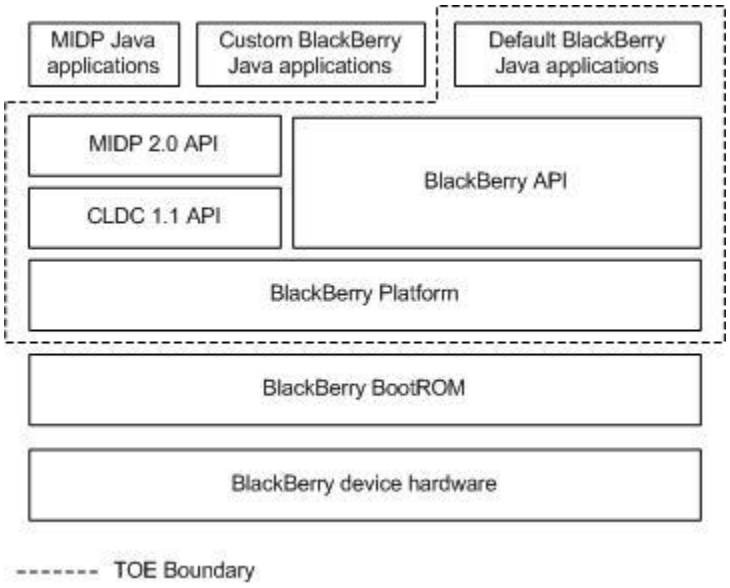

Figure 3. TOE Physical Boundary

1.6.3.2 Logical Boundary

The functionality examined in this evaluation is limited to the following core features of the TOE:

- Secure communication with the BlackBerry Enterprise Server
- Secure communication with other BlackBerry devices
- Remote management of the TOE
- Content protection on the TOE
- File encryption on an external memory device
- Third-party application control
- Wireless communication, including secure S/MIME email messaging
- Wireless PIM data synchronisation
- Management of multimedia applications

2 Conformance Claim

The target of evaluation (TOE) is Part 2 extended, Part 3 conformant, and EAL 4 augmented to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3. 'The EAL 4 augmentation is ALC_FLR.1, Basic flaw remediation.

The TOE is not conformant to a protection profile.

3 Security Problem Definition

3.1 Threats

The following threats are addressed by the TOE:

T.DataDisclosure	Unauthorised entities may monitor and gain access to user data exchanged between the TOE and the BlackBerry Enterprise Server or another BlackBerry device.
T.LossOrTheft	The TOE may be lost or stolen, and an unauthorised individual may attempt to access user data or TOE security functions.
T.ViolatePolicy	The TOE user may inadvertently attempt to manage or use the TOE security functions in violation of the enterprise security policy.

The following threats are addressed by the environment in which the TOE operates:

T.Modify	The TSF-enforcing mechanisms may be modified by an unauthorised individual.

3.2 Organisational Security Policies

The TOE must comply with the following organisational security policies:

P.Provision	The TOE must be provisioned for a specific individual in the enterprise messaging environment by the BlackBerry Enterprise Server administrator prior to use by the individual.
P.Policy	The configuration of the TOE security functions and applications must adhere to the enterprise security policy in conjunction with the Baseline Configuration defined in Section 8.
P.Notify	The TOE user must immediately notify the BlackBerry Enterprise Server administrator if the TOE is lost or stolen.
P.Wireless	The TOE must support wireless PIM data synchronisation and at least the following methods of wireless communication: wireless email, S/MIME email, and SMS messaging; cellular phone communication; and wireless access to the enterprise network and the Internet.
P.TrustedThirdPartyApps	The BlackBerry Enterprise Server administrator shall ensure: - Application control policy is assigned with the Disposition application control policy rule set to Required or Optional for specific, trusted applications only. - Application control policy is assigned with the Disposition application control policy rule set to Disallowed for unspecified or untrusted applications.

3.3 Assumptions

The following assumptions are made about the environment in which the TOE operates:

A.Network	The wireless network required by the TOE is available, and the TOE has permission to use the network.

A.ProperUser	The TOE user is not malicious, attempts to interact with the TOE in compliance with the enterprise security policy, and exercises precautions to reduce the risk of loss or theft of the TOE.

4 Security Objectives

4.1 TOE Security Objectives

The following are the TOE security objectives:

O.DataExchange	The TOE must ensure that all user data exchanged between it and the BlackBerry Enterprise Server or another BlackBerry device is protected from unauthorised disclosure
O.DataStorage	The TOE must provide the capability to protect stored user data from unauthorised disclosure.
O.Admin	The TOE must provide the capability for the TOE user to manage its security functions and execute administrative commands.
O.RemoteAdmin	The TOE must provide the capability for the BlackBerry Enterprise Server administrator to remotely manage the TOE security functions and execute administrative commands.
O.FlexibleAdmin	The remote management capability of the TOE must allow for a high degree of flexibility in managing the TOE security functions.
O.NoOverride	The TOE must prevent the TOE user from overriding the management of security functions performed remotely by the BlackBerry Enterprise Server administrator.
O.Wireless	The TOE must provide the capability to wirelessly synchronise PIM data; send and receive email, S/MIME email, PIN, SMS and MMS messages; send and receive cellular phone communication; access the enterprise network and the Internet; communicate via WiFi and GPS and communicate with Bluetooth devices.

4.2 Environmental Security Objectives

The following security objectives must be met by the environment in which the TOE operates:

O.Network	The TOE must be able to communicate with the BlackBerry Infrastructure.
O.ProperUser	The TOE user must be trusted to interact with the TOE in a manner that maintains its security, complies with the enterprise security policy, and reduces the risk of loss or theft of the TOE.
O.Notify	The TOE user must immediately notify the BlackBerry Enterprise Server administrator if the TOE is lost or stolen.
O.Provision	The BlackBerry Enterprise Server administrator must provision the TOE for the intended TOE user prior to its use.
O.Integrity	The integrity of the TOE must be verified.
O.AdminID	The BlackBerry Enterprise Server must identify authorised users and associate them to an administrative role before permitting them access to BlackBerry Enterprise Server functions or data.

4.3 Security Objectives Rationale

The following table maps the security objectives to the assumptions, threats, and organisational policies identified for the TOE and its environment.

Table 2. Mapping of Security Objectives

	A.Network	A.ProperUser	T.DataDisclosure	T.LossOrTheft	T.ViolatePolicy	T.Modify	P.Provision	P.Policy	P.Notify	P.Wireless	P.TrustedThirdParty Apps
O.DataExchange			X								
O.DataStorage				X							
O.Admin								X			
O.RemoteAdmin				X							
O.FlexibleAdmin								X			
O.NoOverride				X	X						
O.Wireless										X	
O.Network	X										
O.ProperUser		X		X							
O.Notify									X		
O.Provision							X				
O.Integrity						X					
O.AdminID						X					X

4.3.1 A.Network

The O.Network objective ensures the wireless network connectivity required by the TOE exists.

4.3.2 A.ProperUser

The O.ProperUser objective ensures the TOE user is trusted to interact with the TOE in compliance with the enterprise security policy and take precautions to reduce the risk of TOE loss or theft.

4.3.3 T.DataDisclosure

The O.DataExchange objective ensures the user data exchanged between the TOE and the BlackBerry Enterprise Server or another BlackBerry device cannot be disclosed by unauthorised entities.

4.3.4 T.LossOrTheft

The O.DataStorage objective ensures that the TOE may protect stored user data from unauthorised disclosure through the use of cryptographic means or deletion if the TOE is lost or stolen. The O.RemoteAdmin objective ensures that the BlackBerry Enterprise Server administrator may configure the security functions of the TOE and execute administrative commands if the TOE is lost or stolen. The O.NoOverride objective ensures that the TOE user is not able to override the ability of the BlackBerry Enterprise Server administrator to remotely

execute administrative commands if the TOE is lost or stolen. The O.ProperUser objective ensures that the TOE user exercises precautions to reduce the risk of loss or theft.

4.3.5 T.ViolatePolicy

The O.NoOverride objective ensures that the TOE user cannot override the remote management of the TOE security functions performed by the BlackBerry Enterprise Server administrator.

4.3.6 T.Modify

The O.Integrity objective ensures that the TOE has not been modified by an unauthorised individual by verifying the integrity of the TOE. The O.AdminID objective ensures that only authorised users gain access to the BlackBerry Enterprise Server functions and data.

4.3.7 P.Provision

The O.Provision objective ensures that the BlackBerry Enterprise Server administrator provisions the TOE for the intended TOE user prior to its use.

4.3.8 P.Policy

The O.Admin objective ensures that the TOE user can configure the TOE security functions to match the enterprise security policy. The O.FlexibleAdmin objective ensures that there is a high degree of flexibility in remotely managing the TOE security functions so that the TOE complies with the enterprise security policy.

4.3.9 P.Notify

The O.Notify objective ensures that the TOE user immediately notifies the BlackBerry Enterprise Server administrator if the TOE is lost or stolen.

4.3.10 P.Wireless

The O.Wireless objective ensures that the TOE supports the minimum methods of wireless communication.

4.3.11 P.TrustedThirdPartyApps

The O.AdminID objective ensures that only authorised users gain access to the BlackBerry Enterprise Server functions and data.

5 Extended Components Definition

5.1 FCS_VAL_EXP.1 Cryptographic Module Validation

The Common Criteria does not provide an SFR to require that a cryptographic module contained with the TOE boundary meets the requirements of FIPS 140-2. The full statement of FCS_VAL_EXP.1 follows:

FCS_VAL_EXP.1, Cryptographic module validation

FCS_VAL_EXP.1.1 The following cryptographic modules of the TSF shall meet the requirements of FIPS 140-2, *Security Requirements for Cryptographic Modules*: [assignment: *list of cryptographic modules*].

Dependencies: FCS_CKM.4, FCS_COP.1

5.2 FDP_SDP_EXP.1 Stored Data Non-Disclosure

The Common Criteria does not provide an SFR to require that user data be protected from unauthorised disclosure using cryptographic functions. The full statement of FDP_SDP_EXP.1 follows:

FDP_SDP_EXP.1, Stored data non-disclosure

FDP_SDP_EXP.1.1 The TSF shall protect user data stored within the TOE from unauthorised disclosure using [assignment: *cryptographic algorithm*].

Dependencies: FCS_COP.1

5.3 FDP_SDP_EXP.2 Stored Data Deletion

The Common Criteria does not provide an SFR to require that all user data be deleted when specific actions occur. The full statement of FDP_SDP_EXP.2 follows:

FDP_SDP_EXP.2, Stored data deletion

FDP_SDP_EXP.2.1 The TSF shall delete all user data stored within the TOE when the following events occur: [assignment: *events that invoke action*].

Dependencies: None

5.4 FTA_SSL_EXP.4 Event-Initiated Session Locking

The Common Criteria does not provide an SFR to require that an interactive session with the TOE be locked when events other than user invocation or an elapsed time interval occur. The full statement of FTA_SSL_EXP.4 follows:

FTA_SSL_EXP.4, Event-initiated session locking

FTA_SSL_EXP.4.1 The TSF shall lock an interactive session by:

a. clearing or overwriting display devices, making the current contents unreadable;

b. disabling any activity of the user's data access/display devices other than unlocking the session.

when the following events occur: [assignment: *list of events*].

FTA_SSL_EXP.4.2 The TSF shall require the following events to occur prior to unlocking the session: [assignment: *events to occur*].

Dependencies: FIA_UAU.1

6 Security Requirements

This section identifies the security functional and assurance requirements that are applicable to the TOE.

6.1 Conventions

6.1.1 Component Operations

The following typographic conventions are used to identify the permissible operations, as identified in section 8 of CC Part 1, on functional and assurance components:

- Iteration – The iteration operation is identified by enumerating the component. For example, performing the iteration operation on the functional component FMT_MOF.1.1 would result in the component enumeration FMT_MOF.1 (1) and FMT_MOF.1 (2). Functional elements are also enumerated for clarity, for example, FMT_MOF.1.1 (1) and FMT_MOF.1.1 (2).
- Assignment – The assignment operation is identified with regular text contained in brackets. For example, an assignment operation can be performed on FMT_SMR.1.1 as follows: "The TSF shall maintain the roles [root, guest, and user]."
- Selection – The selection operation is identified with italicised text contained in brackets. For example, a selection operation can be performed on FPT_ITT.1.1 as follows: "The TSF shall protect TSF data from [*disclosure*] when it is transmitted between separate parts of the TOE."
- Refinement – The refinement operation is identified with underscored text. For example, a refinement operation can be performed on FTA_TAB.1.1 as follows: "Before establishing a user session, the TSF shall display an advisory warning message that requires acknowledgement by the user regarding unauthorised use of the TOE."

6.1.2 Explicitly Defined Requirements

Explicitly defined functional and assurance requirements are named according to the normal Common Criteria convention with "_EXP" appended. For example, FCS_VAL_EXP.1 is an explicitly defined functional requirement for the FCS, Cryptographic support, functional class.

6.2 Security Functional Requirements

The following functional requirements, listed according to their functional class, are applicable to the TOE.

6.2.1 Class FCS, Cryptographic Support

6.2.1.1 FCS_VAL_EXP.1, Cryptographic module validation

FCS_VAL_EXP.1.1 The following cryptographic modules of the TSF shall meet the requirements of FIPS 140-2, *Security Requirements for Cryptographic Modules*: [

- BlackBerry Cryptographic Kernel Version 3.8.5.85

].

Dependencies: FCS_CKM.4, FCS_COP.1

6.2.1.2 FCS_CKM.1, Cryptographic key generation (1)

FCS_CKM.1.1 (1) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [FIPS 186-2 Appendix 3.1 PRNG] and specified cryptographic key sizes [256 bits, 112 bits] that meet the following: [FIPS 186-2 Appendix 3.1].

Dependencies: [FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2

6.2.1.3 FCS_CKM.1, Cryptographic key generation (2)

FCS_CKM.1.1 (2) The TSF shall generate cryptographic keys in accordance with a specified key generation algorithm [ECDH and ECMQV] and specified cryptographic key sizes [256 bits] that meet the following: [IEEE P1363 Draft 13].

Dependencies: [FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2

6.2.1.4 FCS_CKM.4, Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [zeroization] that meets the following: [FIPS 140-2 zeroization requirements].

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FMT_MSA.2

6.2.1.5 FCS_COP.1, Cryptographic operation

FCS_COP.1.1 The TSF shall perform [data encryption and decryption, random number generation, digital signature verification, and key agreement] in accordance with a specified cryptographic algorithm [

- data encryption and decryption: AES, Triple DES
- random number generation: FIPS 186-2 Appendix 3.1 PRNG
- digital signature verification: ECDSA
- key agreement: ECDH, ECMQV

] and cryptographic key sizes [

- data encryption and decryption: 256 (AES), 192 bits (AES), 112 bits (2-key Triple DES), 128 bits (AES)
- random number generation: not applicable
- digital signature verification: 571 bits
- key agreement: 521 bits[1]

] that meet the following: [

- data encryption and decryption: FIPS 197 (AES), FIPS 46-3 (Triple DES), NIST SP 800-38A (CBC mode of operation)
- random number generation: FIPS 186-2
- digital signature verification: FIPS 186-2, ANSI X9.62-1998
- key agreement: IEEE P1363 Draft 13

[1] The key agreement process results in a 256-bit key for use with AES.

].

Dependencies: [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2

6.2.2 Class FDP, User Data Protection

6.2.2.1 FDP_ACC.1, Subset access control (1)

FDP_ACC.1.1 (1) The TSF shall enforce the [ITPolicy_SFP] on [the application of an IT policy configuration received from a BlackBerry Enterprise Server (per ITCommand_SFP)].

Dependencies: FDP_ACF.1

6.2.2.2 FDP_ACF.1, Security attribute based access control (1)

FDP_ACF.1.1 (1) The TSF shall enforce the [ITPolicy_SFP] to objects based on the following: [attributes for the listed subjects and objects:

- IT command (subject):
  - UID of source BlackBerry Enterprise Server
  - IT command type[2]
  - IT command data[3]
- Current software configuration and IT policy configuration (object):
  - UID of source BlackBerry Enterprise Server
  - ECDSA public key

].

FDP_ACF.1.2 (1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- If there is no current IT policy configuration (i.e. the TOE has not yet been provisioned) then the new IT policy configuration is applied.
- If there is a current IT policy configuration then the new IT policy configuration is applied if the following conditions are satisfied:
  - The UID of the source BlackBerry Enterprise Server for the new and current IT policy configuration match.
  - The ECDSA signature verifies successfully using the ECDSA public key included with the current IT policy configuration.

].

FDP_ACF.1.3 (1) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4 (1) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [none].

Dependencies: FDP_ACC.1, FMT_MSA.3

[2] Per ITCommand_SFP, the IT command type is known to be **Set IT Policy**.
[3] Per ITCommand_SFP, the IT command data is known to contain the new IT policy configuration (which encapsulates the software configuration), an ECDSA public key, an ECDSA signature of the new IT policy configuration and the included ECDSA public key.

6.2.2.3 FDP_ACC.1, Subset access control (2)

FDP_ACC.1.1 (2) The TSF shall enforce the [LocalAdmin_SFP] on [the ability of the TOE user to manage the TSF through the local administration screens].

Dependencies: FDP_ACF.1

6.2.2.4 FDP_ACF.1, Security attribute based access control (2)

FDP_ACF.1.1 (2) The TSF shall enforce the [LocalAdmin_SFP] to objects based on the following: [attributes for the listed subjects and objects:

- TOE user (subject)
- Current IT policy configuration (object)

].

FDP_ACF.1.2 (2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- If the **Password Required** IT policy rule is set to TRUE then the TOE user cannot disable the functionality specified in FIA_UAU.1 and FIA_UID.1.
- If the **User Can Change Timeout** IT policy rule is set to TRUE then the device user can modify the time interval specified in FTA_SSL.1
- If the **User Can Change Timeout** IT policy rule is set to FALSE then the device user cannot modify the time interval specified in FTA_SSL.1
- If the **Disable Bluetooth** IT policy rule is set to FALSE then the device user can enable and disable the flow of Bluetooth communication.
- If the **Disable Bluetooth** IT policy rule is set to TRUE then the device user cannot enable the flow of Bluetooth communication.
- If the **Disable WLAN** IT policy rule is set to FALSE then the device user can enable and disable the flow of WiFi communication.
- If the **Disable WLAN** IT policy rule is set to TRUE then the device user cannot enable the flow of WiFi communication.
- If the **Content Protection Strength** IT policy rule is NULL then the device user can enable and disable the functionality specified in FDP_SDP_EXP.1.
- If the **Content Protection Strength** IT policy rule is not NULL then the device user cannot disable the functionality specified in FDP_SDP_EXP.1.
- If the **Force Lock When Holstered** IT policy rule is set to FALSE then the device user can enable and disable session locking for the device-in-holster event specified in FTA_SSL_EXP.4.
- If the **Force Lock When Holstered** IT policy rule is set to TRUE then the device user cannot disable session locking for the device-in-holster event specified in FTA_SSL_EXP.4.
- If the **S/MIME Allowed Content Ciphers** IT policy rule is NULL then the device user can enable and disable all supported functionality specified in FCS_COP.1.
- If the **S/MIME Allowed Content Ciphers** IT policy rule is not NULL then the device user can enable and disable the designated subset of functionality specified in FCS_COP.1.

- If the **Disable GPS** IT policy rule is set to FALSE then the device user can enable and disable the flow of GPS communication.
- If the **Disable GPS** IT policy rule is set to TRUE then the device user cannot enable the flow of GPS communication.
- If the **Disable JavaScript in Browser** IT policy rule is set to FALSE then the device user can enable the JavaScript.
- If the **Disable JavaScript in Browser** IT policy rule is set to TRUE then the device user cannot enable the JavaScript.
- If the **Disable USB Mass Storage Mode** IT policy rule is set to FALSE then the device user can access an external file system that is connected to the USB port.
- If the **Disable USB Mass Storage Mode** IT policy rule is set to TRUE then the device user cannot access an external file system that is connected to the USB port.
- If the **Set Maximum Password Attempts** IT policy rule is set by administrator to one of the values within the range [3-10] then the device user can change the value to make the configuration more restrictive.

].

FDP_ACF.1.3 (2) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4 (2) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [

- The TOE user can modify the current IT policy configuration to make it more restrictive.

].

Dependencies: FDP_ACC.1, FMT_MSA.3

6.2.2.5 FDP_ACC.1, Subset access control (3)

FDP_ACC.1.1 (3) The TSF shall enforce the [SWConfiguration_SFP] on [the ability of a third party application to access TOE resources and user data].

Dependencies: FDP_ACF.1

6.2.2.6 FDP_ACF.1, Security attribute based access control (3)

FDP_ACF.1.1 (3) The TSF shall enforce the [SWConfiguration_SFP] to objects based on the following: [attributes for the listed subjects and objects:

- Device (subject):
  - Current software configuration
- TOE resources (object):
  - Bluetooth Serial Port Profile API
  - Key store API
  - Input simulation
  - Interprocess communication
  - Authenticator framework API
- User data (object):
  - Email

- Organizer Data
- Files
- Security Data

].

FDP_ACF.1.2 (3) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- If the **BlackBerry Device Keystore** application control policy rule is set to ALLOWED then an application can access the key store APIs on the TOE.
- If the **BlackBerry Device Keystore Medium Security** application control policy rule is set to ALLOWED then an application can access the key store APIs on the TOE.
- If the **Bluetooth Serial Profile** application control policy rule is set to ALLOWED then an application can access the Bluetooth® Serial Port Profile API on the TOE.
- If the **Event Injection** application control policy rule is set to ALLOWED then an application can simulate input events on the TOE, such as pressing keys or performing trackball actions.
- If the **Interprocess Communication** application control policy rule is set to ALLOWED then an application can perform interprocess communication operations.
- If the **Message Access** application control policy rule is set to ALLOWED then an application can send and receive email messages on the TOE.
- If the **PIM Data Access** application control policy rule is set to ALLOWED then an application can access the TOE PIM APIs, which control access to the user's personal information on the TOE, such as the address.
- If the **User Authenticator API** application control policy rule is set to ALLOWED then an application can access the user authenticator framework API.

].

FDP_ACF.1.3 (3) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [none].

FDP_ACF.1.4 (3) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [

The TOE user can modify the current software configuration to make it more restrictive.

].

Dependencies: FDP_ACC.1, FMT_MSA.3

6.2.2.7 FDP_ETC.2, Export of user data with security attributes

FDP_ETC.2.1 The TSF shall enforce the [GME_SFP] when exporting user data, controlled under the SFP(s), outside the TOE to the BlackBerry Infrastructure.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following additional rules when user data is exported from the TSC to the BlackBerry Infrastructure: [none].

Dependencies: [FDP_ACC.1 or FDP_IFC.1]

6.2.2.8 FDP_IFC.1, Subset information flow control (1)

FDP_IFC.1.1 (1) The TSF shall enforce the [GME_SFP] on [all communication to and from the TOE that is routed through the BlackBerry Infrastructure (i.e. all communication between the TOE and a BlackBerry Enterprise Server, and PIN messaging between the TOE and another BlackBerry device)].

Dependencies: FDP_IFF.1

6.2.2.9 FDP_IFF.1, Simple security attributes (1)

FDP_IFF.1.1 (1) The TSF shall enforce the [GME_SFP] based on the following types of subject and information security attributes: [for the listed subjects and information:

- Device (subject):
  - PIN
  - GME service book
  - Current IT policy configuration
- Communication (information):
  - UID of BlackBerry Enterprise Server
  - PIN of remote BlackBerry device

].

FDP_IFF.1.2 (1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- For communication with a BlackBerry Enterprise Server:
  - The PIN of the TOE and the UID of the BlackBerry Enterprise Server must be included in the information sent to the BlackBerry Infrastructure for routing to the BlackBerry Enterprise Server.
- For PIN messaging:
  - Receiving PIN messages is always permitted.
  - If the **Allow Peer-to-Peer Messages** IT policy rule is set to TRUE then sending PIN messages is permitted.
  - The PIN of the TOE and the PIN of the remote device must be included in the information sent to the BlackBerry Infrastructure for routing to the remote device.

].

FDP_IFF.1.3 (1) The TSF shall enforce the following additional rules: [none].

FDP_IFF.1.4 (1) The TSF shall explicitly authorise an information flow based on the following rules [

- For communication with a BlackBerry Enterprise Server:
  - When sending information to a BlackBerry Enterprise Server, the TOE generates a session key and uses it to encrypt the information. The session key is encrypted with the master encryption key and the encrypted information and

encrypted session key are sent to the BlackBerry Infrastructure for routing to the BlackBerry Enterprise Server.

- When receiving information from a BlackBerry Enterprise Server via the BlackBerry Infrastructure, the TOE uses the master encryption key to decrypt the encrypted session key and then uses the session key to decrypt the information.
- Encryption and decryption is performed using the AES algorithm.

- For PIN messaging:
  - When sending a PIN message to another BlackBerry device, the TOE generates a session key and uses it to encrypt the information. The session key is encrypted with the peer-to-peer encryption key and the encrypted information and encrypted session key are sent to the BlackBerry Infrastructure for routing to the remote device.
  - When receiving a PIN message from another BlackBerry device via the BlackBerry Infrastructure, the TOE uses the peer-to-peer encryption key to decrypt the encrypted session key and then uses the session key to decrypt the information.
  - Encryption and decryption is performed using the Triple DES algorithm.

].

FDP_IFF.1.5 (1) The TSF shall explicitly deny an information flow based on the following rules: [none].

6.2.2.10 FDP_IFC.1, Subset information flow control (2)

FDP_IFC.1.1 (2) The TSF shall enforce the [ITCommand_SFP] on [the execution of a wireless IT command received from a BlackBerry Enterprise Server (via the BlackBerry Infrastructure per GME_SFP)].

Dependencies: FDP_IFF.1

6.2.2.11 FDP_IFF.1, Simple security attributes (2)

FDP_IFF.1.1 (2) The TSF shall enforce the [ITCommand_SFP] based on the following types of subject and information security attributes: [for the listed subjects and information:

- IT command (subject):
  - UID of source BlackBerry Enterprise Server
  - Timestamp
  - IT command type
  - IT command data
- Timestamp of previously executed IT command (information)
- Current IT policy configuration (information):
  - UID of source BlackBerry Enterprise Server

].

FDP_IFF.1.2 (2) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- The timestamp of the IT command must be more recent than the timestamp of the previously executed IT command.
- If the IT command type is **Set IT Policy** then the IT command is executed with the supplied IT command data[4] per ITPolicy_SFP.
- If the UID included in the IT command matches the UID in the current IT policy configuration then the IT command is executed, per the following command type:
  - **Erase Data and Disable Handheld** – Performs a security wipe of the device per FDP_SDP_EXP.2.
  - **Set Password and Lock** – Sets the device password to the password specified in the IT command data and locks the device per FTA_SSL_EXP.4.

].

FDP_IFF.1.3 (2) The TSF shall enforce the following additional rules: [none].

- If an IT command is executed then the timestamp of the previously executed IT command is replaced with the timestamp of the current IT command.

].

FDP_IFF.1.4 (2) The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5 (2) The TSF shall explicitly deny an information flow based on the following rules: [

- If the timestamp of the IT command is older than the timestamp of the previously executed IT command then the IT command is not executed.
- If there is no existing IT policy configuration (i.e. the TOE has not yet been provisioned) and the IT command type is not **Set IT Policy** then the IT command is not executed.

].

Dependencies: FDP_IFC.1, FMT_MSA.3

6.2.2.12 FDP_IFC.1, Subset information flow control (3)

FDP_IFC.1.1 (3) The TSF shall enforce the [PIM_SFP] on [the wireless synchronisation of PIM data between the TOE and the corresponding enterprise email account (via a BlackBerry Enterprise Server)].

Dependencies: FDP_IFF.1

6.2.2.13 FDP_IFF.1, Simple security attributes (3)

FDP_IFF.1.1 (3) The TSF shall enforce the [PIM_SFP] based on the following types of subject and information security attributes: [for the listed subjects and information:

- Device (subject):
  - Current IT policy configuration
- PIM data (information)

[4] For the **Set IT Policy** command type, the IT command data contains a new IT policy configuration (which encapsulates the software configuration), an ECDSA public key, and an ECDSA signature of the new IT policy configuration and ECDSA public key.

].

FDP_IFF.1.2 (3) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- If the **Disable All Wireless Sync** IT policy rule is set to FALSE then the wireless synchronisation of PIM data is permitted.

].

FDP_IFF.1.3 (3) The TSF shall enforce the following additional rules: [none].

FDP_IFF.1.4 (3) The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5 (3) The TSF shall explicitly deny an information flow based on the following rules: [

- If the **Disable All Wireless Sync** IT policy rule is set to TRUE then the wireless synchronisation of PIM data is not permitted.

].

Dependencies: FDP_IFC.1, FMT_MSA.3

6.2.2.14 FDP_IFC.1, Subset information flow control (4)

FDP_IFC.1.1 (4) The TSF shall enforce the [ApplicationDownload_SFP] on [downloading and installing third-party applications].

Dependencies: FDP_IFF.1

6.2.2.15 FDP_IFF.1, Simple security attributes (4)

FDP_IFF.1.1 (4) The TSF shall enforce the [ApplicationDownload_SFP] based on the following types of subject and information security attributes: [for the listed subjects and information:

- Device (subject):
  - Current IT policy configuration
  - Current software configuration
- Third-party application (information)

].

FDP_IFF.1.2 (4) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- If the **Disallow Third Party Application Downloads** IT policy rule is set to FALSE then third-party applications may be downloaded and installed.
- If the **Disposition** application control policy rule is set to REQUIRED then third-party application is mandatory and will be downloaded and installed on the TOE. If the control policy rule is set to OPTIONAL then the specific application is considered optional on the TOE, i.e. it can be pushed to the TOE from the BlackBerry Enterprise Server and the user can decide whether or not the application should be removed from the TOE.

].

FDP_IFF.1.3 (4) The TSF shall enforce the following additional rules: [none].

FDP_IFF.1.4 (4) The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5 (4) The TSF shall explicitly deny an information flow based on the following rules: [

- If the **Disallow Third Party Application Downloads** IT policy rule is set to TRUE then third-party applications may not be downloaded and installed.
- If the **Disposition** application control policy rule is set to DISALLOWED then third-party application may not be downloaded and installed.

].

Dependencies: FDP_IFC.1, FMT_MSA.3

6.2.2.16 FDP_IFC.1, Subset information flow control (5)

FDP_IFC.1.1 (5) The TSF shall enforce the [ApplicationFlow_SFP] on [communication initiated by a third-party application with an entity external to the TOE].

Dependencies: FDP_IFF.1

6.2.2.17 FDP_IFF.1, Simple security attributes (5)

FDP_IFF.1.1 (5) The TSF shall enforce the [ApplicationFlow_SFP] based on the following types of subject and information security attributes: [for the listed subjects and information:

- Device (subject):
  - Current IT policy configuration
  - Current software configuration
- Third party application (subject):
- Communication (information):
  - Location of external entity

].

FDP_IFF.1.2 (5) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- If the **Allow External Connections** IT policy rule is set to TRUE then third-party applications are permitted to initiate connections to entities on the external network (e.g. to a public gateway).
- If the **Allow Internal Connections** IT policy rule is set to TRUE then third-party applications are permitted to initiate connections to entities on the internal network (e.g. to the Mobile Data Service of a BlackBerry Enterprise Server).
- If the **Allow Third Party Apps to Use Serial Port** IT policy rule is set to TRUE then third-party applications are permitted to initiate connections to entities through the USB port of the device.
- If the **External Network Connections** application control policy rule is set to PROMPT USER an application prompts the user before it makes external connections through the TOE firewall. If the control policy rule is set to ALLOWED then third-party application can make external network connections through the TOE firewall.

- If the **Internal Network Connections** application control policy rule is set to PROMPT USER an application prompts the user before it makes internal connections through the TOE firewall. If the control policy rule is set to ALLOWED then third-party application can make internal network connections.
- If the **Local Connections** application control policy rule is set to ALLOWED then an application can make local network connections.
- If the **Device GPS** application control policy rule is set to PROMPT USER then an application can access the GPS APIs on the TOE if the user allows it. If the control policy is set to ALLOWED then the application can access the GPS API

].

FDP_IFF.1.3 (5) The TSF shall enforce the following additional rules: [none].

FDP_IFF.1.4 (5) The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5 (5) The TSF shall explicitly deny an information flow based on the following rules: [

- If the **Allow External Connections** IT policy rule is set to FALSE then third-party applications are not permitted to initiate connections to entities on the external network.
- If the **Allow Internal Connections** IT policy rule is set to FALSE then third-party applications are not permitted to initiate connections to entities on the internal network.
- If the **Allow Third Party Apps to Use Serial Port** IT policy rule is set to FALSE then third-party applications are not permitted to initiate connections to entities through the USB port of the device.
- If the **External Network Connections** application control policy rule is set to NOT PERMITTED then third-party application can not make external network connections through the TOE firewall.
- If the **Internal Network Connections** application control policy rule is set to NOT PERMITTED then third-party application can not make internal network connections.
- If the **Local Connections** application control policy rule is set to NOT PERMITTED then an application can not make local network connections.
- If the **Device GPS** application control policy rule is set to NOT PERMITTED then third-party application can not access the GPS APIs.

].

Dependencies: FDP_IFC.1, FMT_MSA.3

6.2.2.18 FDP_IFC.1, Subset information flow control (6)

FDP_IFC.1.1 (6) The TSF shall enforce the [Cellular_SFP] on [cellular phone communication, SMS messaging, MMS messaging].

Dependencies: FDP_IFF.1

6.2.2.19 FDP_IFF.1, Simple security attributes (6)

FDP_IFF.1.1 (6) The TSF shall enforce the [Cellular_SFP] based on the following types of subject and information security attributes: [for the listed subjects and information:

- Device (subject):
  - Current IT policy configuration
  - Current software configuration
- Cellular phone communication (information)
- SMS messages (information)
- MMS messages (information)

].

FDP_IFF.1.2 (6) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- If the **Allow Phone** IT policy rule is set to TRUE then cellular phone communication is permitted.
- If the **Allow SMS** IT policy rule is set to TRUE then SMS messaging is permitted.
- If the **Disable MMS** IT policy rule is set to FALSE then MMS messaging is permitted.
- If the **Phone Access** application control policy rule is set to PROMPT USER then an application can make calls and access call logs on the TOE if the user allows it. If the control policy rule is set to ALLOWED then an application can make calls and access call logs on the TOE.

].

FDP_IFF.1.3 (6) The TSF shall enforce the following additional rules: [none].

FDP_IFF.1.4 (6) The TSF shall explicitly authorise an information flow based on the following rules: [

- Cellular phone communication to emergency numbers (e.g. 911) is always permitted.

].

FDP_IFF.1.5 (6) The TSF shall explicitly deny an information flow based on the following rules: [

- If the **Allow Phone** IT policy rule is set to FALSE then cellular phone communication is not permitted.
- If the **Allow SMS** IT policy rule is set to FALSE then SMS messaging is not permitted.
- If the **Disable MMS** IT policy rule is set to TRUE then MMS messaging is not permitted.
- If the **Phone Access** application control policy rule is set to NOT PERMITTED then an application can not make calls and access call logs on the TOE.

].

Dependencies: FDP_IFC.1, FMT_MSA.3

6.2.2.20 FDP_IFC.1, Subset information flow control (7)

FDP_IFC.1.1 (7) The TSF shall enforce the [Radio_SFP] on [Bluetooth communication, WiFi communication and GPS communication].

Dependencies: FDP_IFF.1

6.2.2.21 FDP_IFF.1, Simple security attributes (7)

FDP_IFF.1.1 (7) The TSF shall enforce the [Radio_SFP] based on the following types of subject and information security attributes: [

- Device (subject):
  - Current IT policy configuration
- Bluetooth communication (information)
- WiFi communication (information)
- GPS communication (information)

].

FDP_IFF.1.2 (7) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- If the **Disable Bluetooth** IT policy rule is set to FALSE then Bluetooth communication is permitted.
- If the **Disable WLAN** IT policy rule is set to FALSE then WiFi communication is permitted.
- If the **Disable GPS** IT policy rule is set to FALSE then GPS communication is permitted.

].

FDP_IFF.1.3 (7) The TSF shall enforce the following additional rules: [none].

FDP_IFF.1.4 (7) The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5 (7) The TSF shall explicitly deny an information flow based on the following rules: [

- If the **Disable Bluetooth** IT policy rule is set to TRUE then Bluetooth communication is not permitted.
- If the **Disable WLAN** IT policy rule is set to TRUE then WiFi communication is not permitted.
- If the **Disable GPS** IT policy rule is set to TRUE then GPS communication is not permitted.

].

Dependencies: FDP_IFC.1, FMT_MSA.3

6.2.2.22 FDP_IFC.1, Subset information flow control (8)

FDP_IFC.1.1 (8) The TSF shall enforce the [Multimedia_SFP] on [multimedia applications].

Dependencies: FDP_IFF.1

6.2.2.23 FDP_IFF.1, Simple security attributes (8)

FDP_IFF.1.1 (8) The TSF shall enforce the [Multimedia_SFP] based on the following types of subject and information security attributes: [

- Device (subject):

    - Current IT policy configuration
- Multimedia application (information)

].

FDP_IFF.1.2 (8) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- If the **Disable Voice Note Recording** IT policy rule is set to FALSE then voice note recording is permitted.
- If the **Disable Photo Camera** IT policy rule is set to FALSE then taking pictures is permitted.
- If the **Disable Video Camera** IT policy rule is set to FALSE then video recording is permitted.
- If the **Disable External Memory** IT policy rule is set to FALSE then storing data on the external memory is permitted.
- If the **Disable USB Mass Storage** IT policy rule is set to FALSE then using of an external file system connected to the USB port is permitted.

].

FDP_IFF.1.3 (8) The TSF shall enforce the following additional rules: [none].

FDP_IFF.1.4 (8) The TSF shall explicitly authorise an information flow based on the following rules: [none].

FDP_IFF.1.5 (8) The TSF shall explicitly deny an information flow based on the following rules: [

- If the **Disable Voice Note Recording** IT policy rule is set to TRUE then voice note recording is not permitted.
- If the **Disable Photo Camera** IT policy rule is set to TRUE then taking pictures is not permitted.
- If the **Disable Video Camera** IT policy rule is set to TRUE then video recording is not permitted.
- If the **Disable External Memory** IT policy rule is set to TRUE then storing data on the external memory is not permitted.
- If the **Disable USB Mass Storage** IT policy rule is set to TRUE then using of an external file system connected to the USB port is not permitted.

].

Dependencies: FDP_IFC.1, FMT_MSA.3

6.2.2.24 FDP_ITC.2, Import of user data with security attributes

FDP_ITC.2.1 The TSF shall enforce the [GME_SFP] when importing user data, controlled under the SFP, from the BlackBerry Infrastructure.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following additional rules when importing user data controlled under the SFP from the BlackBerry Infrastructure: [none].

Dependencies: [FDP_ACC.1 or FDP_IFC.1], [FTP_ITC.1 or FTP_TRP.1], FPT_TDC.1

6.2.2.25 FDP_SDP_EXP.1, Stored data non-disclosure

FDP_SDP_EXP.1.1 The TSF shall protect user data stored within the TSC from unauthorised disclosure using [AES-256].

Dependencies: FCS_COP.1

6.2.2.26 FDP_SDP_EXP.2, Stored data deletion

FDP_SDP_EXP.2.1 The TOE shall delete all user data stored within the TSC when the following events occur: [

- The **Erase Data and Disable Handheld** IT command is received per ITCommand_SFP.
- The device user invokes a security wipe per FMT_SMF.1.
- The maximum number of unsuccessful authentication attempts is reached per FIA_AFL.1.

].

Dependencies: None.

6.2.3 Class FIA, Identification and Authentication

6.2.3.1 FIA_AFL.1, Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [*a configurable positive integer within [3 and 10]*] unsuccessful authentication attempts occur related to [the number of unsuccessful authentication attempts since the last successful authentication].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [perform a security wipe of all user data].

Dependencies: FIA_UAU.1

6.2.3.2 FIA_SOS.1, Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [a combination of the following metrics:

- The minimum length of the device password must be a BlackBerry Enterprise Server administrator configurable number between 4 and 14.
- The character composition of the device password must satisfy one of the following conditions chosen by the BlackBerry Enterprise Server administrator:
    - Contain at least one alpha and one numeric character
    - Contain at least one alpha, one numeric, and one special character

- Contain at least one uppercase alpha, one lowercase alpha, one numeric, and one special character

- The device password cannot match a BlackBerry Enterprise Server administrator configurable number between 1 and 15 previous device passwords.

].

Dependencies: None

6.2.3.3 FIA_UAU.1, Timing of authentication

FIA_UAU.1.1 The TSF shall allow [the following actions:

- Display general status information (e.g. battery level, date, time, number of unread messages)
- Receive email, SMS, MMS and PIN messages
- Receive calendar appointments
- Synchronise PIM data
- Receive cellular phone communication
- Send emergency cellular phone communication (e.g. 911)

] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1

6.2.3.4 FIA_UAU.7, Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide only [an asterisk for each character typed] to the user while authentication is in progress.

Dependencies: FIA_UAU.1

6.2.3.5 FIA_UID.1, Timing of identification

FIA_UID.1.1 The TSF shall allow [the actions specified in FIA_UAU.1.1] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: None

6.2.4 Class FMT, Security Management

6.2.4.1 FMT_MSA.1, Management of security attributes (1)

FMT_MSA.1.1 (1) The TSF shall enforce the [ITCommand_SFP and ITPolicy_SFP] to restrict the ability to [*modify*] the security attributes [IT command type and data] to [the BlackBerry Enterprise Server administrator].

Dependencies: [FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1, FMT_SMR.1

6.2.4.2 FMT_MSA.1, Management of security attributes (2)

FMT_MSA.1.1 (2) The TSF shall enforce the [LocalAdmin_SFP, PIM_SFP, ApplicationDownload_SFP, ApplicationFlow_SFP, Cellular_SFP, Multimedia_SFP and Radio_SFP] to restrict the ability to [*modify*] the security attributes [current IT policy configuration] to [the BlackBerry Enterprise Server administrator].

Dependencies: [FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1, FMT_SMR.1

6.2.4.3 FMT_MSA.1, Management of security attributes (3)

FMT_MSA.1.1 (3) The TSF shall enforce the [GME_SFP] to restrict the ability to [*modify*] the security attributes [current IT policy configuration and GME service book] to [the BlackBerry Enterprise Server administrator].

Dependencies: [FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1, FMT_SMR.1

6.2.4.4 FMT_MSA.1, Management of security attributes (4)

FMT_MSA.1.1 (4) The TSF shall enforce the [LocalAdmin_SFP and SWConfiguraion_SFP] to restrict the ability to [*modify*] the security attributes [software configuration] to [the BlackBerry Enterprise Server administrator].

Dependencies: [FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1, FMT_SMR.1

6.2.4.5 FMT_MSA.2, Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Dependencies: [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1

6.2.4.6 FMT_MSA.3, Static attribute initialisation (1)

FMT_MSA.3.1 (1) The TSF shall enforce the [ITPolicy_SFP] to provide [*permissive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (1) The TSF shall allow the [BlackBerry Enterprise Server administrator] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1, FMT_SMR.1

6.2.4.7 FMT_MSA.3, Static attribute initialisation (2)

FMT_MSA.3.1 (2) The TSF shall enforce the [LocalAdmin_SFP] to provide [*permissive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (2) The TSF shall allow the [BlackBerry Enterprise Server administrator] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1, FMT_SMR.1

6.2.4.8 FMT_MSA.3, Static attribute initialisation (3)

FMT_MSA.3.1 (3) The TSF shall enforce the [GME_SFP] to provide [*permissive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (3) The TSF shall allow the [BlackBerry Enterprise Server administrator] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1, FMT_SMR.1

6.2.4.9 FMT_MSA.3, Static attribute initialisation (4)

FMT_MSA.3.1 (4) The TSF shall enforce the [ITCommand_SFP] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (4) The TSF shall allow the [BlackBerry Enterprise Server administrator] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1, FMT_SMR.1

6.2.4.10 FMT_MSA.3, Static attribute initialisation (5)

FMT_MSA.3.1 (5) The TSF shall enforce the [PIM_SFP, ApplicationDownload_SFP, ApplicationFlow_SFP, Cellular_SFP, Multimedia_SFP and Radio_SFP] to provide [*permissive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (5) The TSF shall allow the [BlackBerry Enterprise Server administrator] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1, FMT_SMR.1

6.2.4.11 FMT_MSA.3, Static attribute initialisation (6)

FMT_MSA.3.1 (6) The TSF shall enforce the [SWConfiguration_SFP] to provide [*permissive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 (6) The TSF shall allow the [BlackBerry Enterprise Server administrator] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1, FMT_SMR.1

6.2.4.12 FMT_SAE.1, Time-limited authorisation

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [

- Device password (between 1 and 65535 days)

] to [the BlackBerry Enterprise Server administrator].

FMT_SAE.1.2 For each of the security attributes, the TSF shall be able to [

- Device password – force the user to change the password

] after the expiration time for the indicated security attribute has passed.

Dependencies: FMT_SMR.1, FPT_STM.1

6.2.4.13 FMT_SMF.1, Specification of management functions

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [

- On behalf of the device user:
  - Enable and disable the functionality specified in FDP_SDP_EXP.1 (unless prevented per LocalAdmin_SFP)
  - Set the time interval for FTA_SSL.1 (unless prevented per LocalAdmin_SFP)
  - Enable and disable session locking when the device is placed in its holster per FTA_SSL_EXP.4 (unless prevented per LocalAdmin_SFP)
  - Cooperatively generate a new master encryption key with the BlackBerry Enterprise Server
  - Perform a security wipe of the device per FDP_SDP_EXP.2
  - Enable and disable Bluetooth functionality (unless prevented per LocalAdmin_SFP)
  - Enable and disable WiFi functionality (unless prevented per LocalAdmin_SFP)
  - Modify the device password
  - Enable and disable GPS functionality (unless prevented per LocalAdmin_SFP)
  - Enable or disable file encryption on an external memory
  - Enable or disable mass storage mode
- On behalf of the BlackBerry Enterprise Server administrator:
  - Modify the peer-to-peer encryption key
  - Inject a new GME service book
  - Lock the TOE session and set the device password
  - Perform a security wipe of the device per FDP_SDP_EXP.2
  - Modify the device password
  - Apply an IT policy configuration to perform one or more of the following management functions:
    - Enable and disable the functionality specified in FDP_SDP_EXP.1
    - Configure the password length, pattern checks, and history per FIA_SOS.1
    - Enable and disable the password history per FIA_SOS.1
    - Enable and disable the functionality specified in FMT_SAE.1
    - Set the maximum time interval for FTA_SSL.1
    - Set the time interval for FTA_SSL.1

- Enable and disable session locking when the device is placed in its holster per FTA_SSL_EXP.4
- Configure the behaviour specified in PIM_SFP, ApplicationDownload_SFP, ApplicationFlow_SFP, Cellular_SFP, Multimedia_SFP and Radio_SFP

- Apply a software configuration to perform the following management functions:
  - Configure the behaviour specified in SWConfiguraion_SFP

].

Dependencies: None

6.2.5 Class FPT, Protection of the TSF

6.2.5.1 FPT_STM.1, Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

Dependencies: None

6.2.5.2 FPT_TDC.1, Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [all data] when shared between the TSF and the BlackBerry Infrastructure.

FPT_TDC.1.2 The TSF shall use [the GME specification] when interpreting the TSF data from the BlackBerry Infrastructure.

Dependencies: None

6.2.6 Class FTA, TOE Access

6.2.6.1 FTA_SSL.1, TSF-initiated session locking

FTA_SSL.1.1 The TSF shall lock an interactive session after [a time interval of inactivity configurable per ITPolicy_SFP and LocalAdmin_SFP] by:

a. clearing or overwriting display devices, making the current contents unreadable;

b. disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [user authentication].

Dependencies: FIA_UAU.1

6.2.6.2 FTA_SSL.2, User-initiated locking

FTA_SSL.2.1 The TSF shall allow user-initiated locking of the user's own interactive session by:

a. clearing or overwriting display devices, making the current contents unreadable;

b. disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.2.2 The TSF shall require the following events to occur prior to unlocking the session: [user authentication].

Dependencies: FIA_UAU.1

6.2.6.3 FTA_SSL_EXP.4, Event-initiated session locking

FTA_SSL_EXP.4.1 The TSF shall lock an interactive session by:

a. clearing or overwriting display devices, making the current contents unreadable;

b. disabling any activity of the user's data access/display devices other than unlocking the session.

when the following events occur: [

- The device is placed in its holster, if so configured per LocalAdmin_SFP.
- The **Set Password and Lock** IT command is received per ITCommand_SFP.

].

FTA_SSL_EXP.4.2 The TSF shall require the following events to occur prior to unlocking the session: [user authentication].

Dependencies: FIA_UAU.1

6.2.7 Class FTP, Trusted Path / Channels

6.2.7.1 FTP_ITC.1, Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and the BlackBerry Infrastructure that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [*the TSF*, *the* BlackBerry Infrastructure] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [sending data to a BlackBerry Enterprise Server or another device].

Dependencies: None

6.3 Security Assurance Requirements

6.3.1 Selection of Security Assurance Requirements

The selection of EAL 4 assurance package is commensurate with the protected environment in which the TOE executes, and the augmentation of ALC_FLR.1 is appropriate to provide assurance to consumers that security flaws are tracked and corrected.

The assurance requirements for the TOE are specified by the assurance components in the following table. The components are taken from Part 3 of the Common Criteria and are EAL 4 augmented, with augmented components listed in bold text.

Table 3. TOE Assurance Components

Assurance Class	Assurance Components
Security Target evaluation	ASE_CCL.1, Conformance claims
	ASE_ECD.1, Extended components definition
	ASE_INT.1, ST introduction
	ASE_OBJ.2, Security objectives
	ASE_REQ.2, Derived security requirements
	ASE_SPD.1, Security problem definition
	ASE_TSS.1, TOE summary specification
Development	ADV_FSP.4, Complete functional specification
	ADV_TDS.3, Basic modular design
	ADV_ARC.1, Security architecture description
	ADV_IMP.1, Implementation representation of the TSF
Guidance documents	AGD_OPE.1, Operational user guidance
	AGD_PRE.1, Preparative procedures
Life cycle support	**ALC_FLR.1, Basic flaw remediation**
	ALC_CMC.4, Production support, acceptance procedures and automation
	ALC_CMS.4, Problem tracking CM coverage
	ALC_DEL.1, Delivery procedures
	ALC_DVS.1, Identification of security measures
	ALC_LCD.1, Developer defined life-cycle model
	ALC_TAT.1, Well-defined development tools
Tests	ATE_COV.2, Analysis of coverage
	ATE_FUN.1, Functional testing
	ATE_IND.2, Independent testing – sample
	ATE_DPT.2, Testing: security enforcing modules
Vulnerability assessment	AVA_VAN.3, Focused vulnerability analysis

6.4 Security Requirements Rationale

6.4.1 Satisfaction of Security Objectives

The following table maps the SFRs to the security objectives for the TOE and its environment.

Table 4. Mapping of SFRs to Security Objectives

	O.DataExchange	O.DataStorage	O.Admin	O.RemoteAdmin	O.FlexibleAdmin	O.NoOverride	O.Wireless
FCS_VAL_EXP.1	X	X					
FCS_CKM.1 (1)	X	X					
FCS_CKM.1 (2)	X	X					
FCS_CKM.4	X	X					
FCS_COP.1	X	X					X
FDP_ACC.1 (1)				X			
FDP_ACF.1 (1)				X			
FDP_ACC.1 (2)						X	
FDP_ACF.1 (2)						X	
FDP_ACC.1 (3)						X	
FDP_ACF.1 (3)						X	
FDP_ETC.2	X						
FDP_IFC.1 (1)	X			X			X
FDP_IFF.1 (1)	X			X			X
FDP_IFC.1 (2)				X			
FDP_IFF.1 (2)				X			
FDP_IFC.1 (3)				X			X
FDP_IFF.1 (3)				X			X
FDP_IFC.1 (4)				X			
FDP_IFF.1 (4)				X			
FDP_IFC.1 (5)				X			X
FDP_IFF.1 (5)				X			X
FDP_IFC.1 (6)				X			X
FDP_IFF.1 (6)				X			X
FDP_IFC.1 (7)				X			X
FDP_IFF.1 (7)				X			X
FDP_IFC.1 (8)		X		X			X
FDP_IFF.1 (8)		X		X			X
FDP_ITC.2	X						
FDP_SDP_EXP.1		X					
FDP_SDP_EXP.2		X					
FIA_AFL.1					X		
FIA_SOS.1					X		
FIA_UAU.1					X		

	O.DataExchange	O.DataStorage	O.Admin	O.RemoteAdmin	O.FlexibleAdmin	O.NoOverride	O.Wireless
FIA_UAU.7					X		
FIA_UID.1					X		
FMT_MSA.1 (1)				X		X	
FMT_MSA.1 (2)				X		X	
FMT_MSA.1 (3)				X		X	
FMT_MSA.1 (4)				X		X	
FMT_MSA.2	X	X					
FMT_MSA.3 (1)				X			
FMT_MSA.3 (2)						X	
FMT_MSA.3 (3)				X			
FMT_MSA.3 (4)				X			
FMT_MSA.3 (5)				X			
FMT_MSA.3 (6)				X			
FMT_SAE.1					X		
FMT_SMF.1			X	X	X	X	
FPT_STM.1					X		
FPT_TDC.1	X						
FTA_SSL.1					X		
FTA_SSL.2			X				
FTA_SSL_EXP.4					X		
FTP_ITC.1	X						

6.4.1.1 O.DataExchange

FCS_CKM.1 (1), FCS_CKM.1 (2), FCS_CKM.4 and FCS_COP.1 ensure that the TOE implements the cryptographic functionality required to generate and destroy keys and encrypt and decrypt data. FCS_VAL_EXP.1 ensures that the cryptographic operations are implemented correctly.

FDP_IFC.1 (1) and FDP_IFF.1 (1) ensure that the TOE encrypts and decrypts data sent to and received from a BlackBerry Enterprise Server or another BlackBerry device.

FMT_MSA.2 ensures that only secure values can be used for cryptographic operations.

FDP_ETC.2, FDP_ITC.2, and FPT_TDC.1 ensure that the security attributes of the user data is correctly handled between the TOE and the BlackBerry Infrastructure.

FDP_ITC.1 ensures that the communication channel between the TOE and the BlackBerry Infrastructure is logically distinct.

6.4.1.2 O.DataStorage

FCS_CKM.1 (1), FCS_CKM.1 (2), FCS_CKM.4 and FCS_COP.1 ensure that the TOE implements the cryptographic functionality required to generate and destroy keys and encrypt and decrypt data. FCS_VAL_EXP.1 ensures that the cryptographic operations are implemented correctly.

FDP_IFC.1.1 (8), FDP_IFF.1.1 (8) and FDP_SDP_EXP.1 ensures that stored user data is protected from unauthorised disclosure using cryptographic means, and FDP_SDP_EXP.2 ensures that all stored user data can be deleted to prevent disclosure.

FMT_MSA.2 ensures that only secure values can be used for cryptographic operations.

6.4.1.3 O.Admin

FMT_SMF.1 ensures that the TOE user can manage the TOE security functions.

FTA_SSL.2 ensures that the TOE user can lock the session with the TOE.

6.4.1.4 O.RemoteAdmin

FDP_ACC.1 (1), FDP_ACF.1 (1), FMT_MSA.1 (1), and FMT_MSA.3 (1) ensure that the BlackBerry Enterprise Server administrator can remotely manage the TOE security functions by issuing an IT policy configuration.

FDP_IFC.1 (1) and FDP_IFF.1 (1) ensure that the BlackBerry Enterprise Server administrator can remotely manage the communication between the TOE and the BlackBerry Enterprise Server.

FDP_IFC.1 (2), FDP_IFF.1 (2), FMT_MSA.1 (1), and FMT_MSA.3 (4) ensure that the BlackBerry Enterprise Server administrator can remotely manage the TOE security functions by issuing IT commands.

FDP_IFC.1 (3), FDP_IFF.1 (3), FMT_MSA.1 (2), and FMT_MSA.3 (5) ensure that the BlackBerry Enterprise Server administrator can manage the flow of PIM data to and from the TOE.

FDP_IFC.1 (4), FDP_IFF.1 (4), FMT_MSA.1 (2), and FMT_MSA.3 (5) ensure that the BlackBerry Enterprise Server administrator can manage the downloading of third-party applications to the TOE.

FDP_IFC.1 (5), FDP_IFF.1 (5), FMT_MSA.1 (2), and FMT_MSA.3 (5) ensure that the BlackBerry Enterprise Server administrator can manage the flow of data to and from third-party applications on the TOE.

FDP_IFC.1 (6), FDP_IFF.1 (6), FMT_MSA.1 (2), and FMT_MSA.3 (5) ensure that the BlackBerry Enterprise Server administrator can manage the flow of cellular phone communication, SMS messaging and MMS messaging to and from the TOE.

FDP_IFC.1 (7), FDP_IFF.1 (7), FMT_MSA.1 (2), and FMT_MSA.3 (5) ensure that the BlackBerry Enterprise Server administrator can manage the flow of Bluetooth, WiFi and GPS communication to and from the TOE.

FDP_IFC.1 (8), FDP_IFF.1 (8), FMT_MSA.1 (2), and FMT_MSA.3 (5) ensure that the BlackBerry Enterprise Server administrator can manage the multimedia applications, including camera, video recorder, voice note recorder and multimedia data storage on external memory.

FMT_SMF.1 ensures that the BlackBerry Enterprise Server administrator can manage the security functions of the TOE.

FMT_MSA.1 (4), and FMT_MSA.3 (6) ensure that the BlackBerry Enterprise Server administrator can remotely manage the TOE security functions by issuing a software configuration.

6.4.1.5 O.FlexibleAdmin

FMT_SMF.1, FIA_AFL.1, FIA_UAU.1, FIA_UAU.7, FIA_UID.1, FTA_SSL.1, and FTA_SSL_EXP.4 ensure that the BlackBerry Enterprise Server administrator can manage the TOE authentication mechanism to comply with the enterprise security policy.

FMT_SMF.1, FIA_SOS.1, FMT_SAE.1, and FPT_STM.1 ensure that the BlackBerry Enterprise Server administrator can configure the TOE password handling to comply with the enterprise security policy.

6.4.1.6 O.NoOverride

FDP_ACC.1 (2), FDP_ACC.1 (3), FDP_ACF.1 (2) and FDP_ACF.1 (3) ensure that the TOE user cannot override the management of security functions performed by the BlackBerry Enterprise Server administrator.

FMT_MSA.1 (1), FMT_MSA.1 (2), FMT_MSA.1 (3), FMT_MSA.1 (4), FMT_MSA.3 (2), and FMT_SMF.1 ensure that the BlackBerry Enterprise Server administrator can specify which security functions can be managed by the TOE user.

6.4.1.7 O.Wireless

FDP_IFC.1 (1), FDP_IFF.1 (1) and FCS_COP.1 (2) ensure that the TOE supports wireless email and PIN messaging.

FDP_IFC.1 (3) and FDP_IFF.1 (3) ensure that the TOE supports wireless PIM data synchronisation.

FDP_IFC.1 (5) and FDP_IFF.1 (5) ensure that the TOE supports wireless access to the enterprise network and the Internet.

FDP_IFC.1 (6) and FDP_IFF.1 (6) ensure that the TOE supports cellular phone communication, SMS messaging and MMS messaging.

FDP_IFC.1 (7) and FDP_IFF.1 (7) ensure that the TOE supports communication with Bluetooth, WiFi and GPS devices.

FDP_IFC.1 (8) and FDP_IFF.1 (8) ensure that the TOE supports multimedia applications, including photo camera, video camera, external memory and voice notes recording.

6.4.2 Dependencies of Security Functional Requirements

The following table demonstrates that each SFR dependency is either satisfied or sufficient rationale provided.

Table 5. SFR Dependencies

Requirement	Dependencies	Satisfied By
FCS_VAL_EXP.1	FCS_CKM.4	FCS_CKM.4
	FCS_COP.1	FCS_COP.1
FCS_CKM.1 (1)	FCS_CKM.2 or FCS_COP.1	FCS_COP.1
	FCS_CKM.4	FCS_CKM.4
	FMT_MSA.2	FMT_MSA.2
FCS_CKM.1 (2)	FCS_CKM.2 or FCS_COP.1	FCS_COP.1
	FCS_CKM.4	FCS_CKM.4
	FMT_MSA.2	FMT_MSA.2

Requirement	Dependencies	Satisfied By
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1 (1), FCS_CKM.1 (2)
	FMT_MSA.2	FMT_MSA.2
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1 (1), FCS_CKM.1 (2), FDP_ITC.1
	FCS_CKM.4	FCS_CKM.4
	FMT_MSA.2	FMT_MSA.2
FDP_ACC.1 (1)	FDP_ACF.1	FDP_ACF.1 (1)
FDP_ACF.1 (1)	FDP_ACC.1	FDP_ACC.1 (1)
	FMT_MSA.3	FMT_MSA.3 (1)
FDP_ACC.1 (2)	FDP_ACF.1	FDP_ACF.1 (2)
FDP_ACF.1 (2)	FDP_ACC.1	FDP_ACC.1 (2)
	FMT_MSA.3	FMT_MSA.3 (2)
FDP_ACC.1 (3)	FDP_ACF.1	FDP_ACF.1 (4)
FDP_ACF.1 (3)	FDP_ACC.1	FDP_ACC.1 (4)
	FMT_MSA.3	FMT_MSA.3 (2)
FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1	FDP_IFC.1 (1)
FDP_IFC.1 (1)	FDP_IFF.1	FDP_IFF.1 (1)
FDP_IFF.1 (1)	FDP_IFC.1	FDP_IFC.1 (1)
	FMT_MSA.3	FMT_MSA.3 (3)
FDP_IFC.1 (2)	FDP_IFF.1	FDP_IFF.1 (2)
FDP_IFF.1 (2)	FDP_IFC.1	FDP_IFC.1 (2)
	FMT_MSA.3	FMT_MSA.3 (4)
FDP_IFC.1 (3)	FDP_IFF.1	FDP_IFF.1 (3)
FDP_IFF.1 (3)	FDP_IFC.1	FDP_IFC.1 (3)
	FMT_MSA.3	FMT_MSA.3 (5)
FDP_IFC.1 (4)	FDP_IFF.1	FDP_IFF.1 (4)
FDP_IFF.1 (4)	FDP_IFC.1	FDP_IFC.1 (4)
	FMT_MSA.3	FMT_MSA.3 (5)
FDP_IFC.1 (5)	FDP_IFF.1+	FDP_IFF.1 (5)
FDP_IFF.1 (5)	FDP_IFC.1	FDP_IFC.1 (5)
	FMT_MSA.3	FMT_MSA.3 (5)
FDP_IFC.1 (6)	FDP_IFF.1	FDP_IFF.1 (6)
FDP_IFF.1 (6)	FDP_IFC.1	FDP_IFC.1 (6)
	FMT_MSA.3	FMT_MSA.3 (5)
FDP_IFC.1 (7)	FDP_IFF.1	FDP_IFF.1 (8)
FDP_IFF.1 (7)	FDP_IFC.1	FDP_IFC.1 (8)
	FMT_MSA.3	FMT_MSA.3 (5)
FDP_IFC.1 (8)	FDP_IFF.1	FDP_IFF.1 (10)

Requirement	Dependencies	Satisfied By
FDP_IFF.1 (8)	FDP_IFC.1	FDP_IFC.1 (10)
	FMT_MSA.3	FMT_MSA.3 (5)
FDP_ITC.2	FDP_ACC.1 or FDP_IFC.1	FDP_IFC.1 (1)
	FTP_ITC.1 or FTP_TRP.1	FTP_ITC.1
	FPT_TDC.1	FPT_TDC.1
FDP_SDP_EXP.1	FCS_COP.1	FCS_COP.1
FDP_SDP_EXP.2	None	–
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_SOS.1	None	–
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	None	–
FMT_MSA.1 (1)	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1 (1), FDP_IFC.1 (2)
	FMT_SMF.1	FMT_SMF.1
	FMT_SMR.1	FMT_SMR.1 (ENV)
FMT_MSA.1 (2)	FDP_ACC.1 or FDP_IFC.1	FDP_IFC.1 (3) , FDP_IFC.1 (4) , FDP_IFC.1 (5) , FDP_IFC.1 (6) , FDP_IFC.1 (7) , FDP_IFC.1 (8)
	FMT_SMF.1	FMT_SMF.1
	FMT_SMR.1	environment, security objective for OE
FMT_MSA.1 (3)	FDP_ACC.1 or FDP_IFC.1	FDP_IFC.1 (1)
	FMT_SMF.1	FMT_SMF.1
	FMT_SMR.1	environment, security objective for OE
FMT_MSA.1 (4)	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1 (3)
	FMT_SMF.1	FMT_SMF.1
	FMT_SMR.1	environment, security objective for OE
	FDP_ACC.1 or FDP_IFC.1	Not applicable[5]
	FMT_MSA.1	Not applicable[6]
	FMT_SMR.1	Not applicable[6]
FMT_MSA.3 (1)	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	environment, security objective for OE
FMT_MSA.3 (2)	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	environment, security objective for OE
FMT_MSA.3 (3)	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	environment, security objective for OE

[5] The TSF automatically generates symmetric keys and performs encryption and decryption as needed and does not require input or administration from the TOE user. Similarly, digital signature verification is performed automatically. Consequently, the dependencies on FDP_ACC.1 (or FDP_IFC.1), FMT_MSA.1, and FMT_SMR.1 are not applicable.

Requirement	Dependencies	Satisfied By
FMT_MSA.3 (4)	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	environment, security objective for OE
FMT_MSA.3 (5)	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	environment, security objective for OE
FMT_MSA.3 (6)	FMT_MSA.1	FMT_MSA.1
	FMT_SMR.1	environment, security objective for OE
FMT_SAE.1	FMT_SMR.1	environment, security objective for OE
	FPT_STM.1	FPT_STM.1
FMT_SMF.1	None	–
FPT_STM.1	None	–
FPT_TDC.1	None	–
FTA_SSL.1	FIA_UAU.1	FIA_UAU.1
FTA_SSL.2	FIA_UAU.1	FIA_UAU.1
FTA_SSL_EXP.4	FIA_UAU.1	FIA_UAU.1
FTP_ITC.1	None	–

6.4.3 Refinements of Security Functional Requirements on the TOE

6.4.3.1 FDP_ACF.1 (1) Security Attribute Based Access Control

In FDP_ACF.1.4 (1) “based on the” was changed to “based on the following additional rules” to improve legibility and does not affect the meaning of the functional requirement.

6.4.3.2 FDP_ACF.1 (2) Security Attribute Based Access Control

In FDP_ACF.1.4 (2) “based on the” was changed to “based on the following additional rules” to improve legibility and does not affect the meaning of the functional requirement.

6.4.3.3 FDP_ETC.2 Export of User Data with Security Attributes

The GME_SFP is only applicable for communication between the TOE and the BlackBerry Infrastructure, thus “to the BlackBerry Infrastructure” was added FDP_ETC.2.1 and FDP_ETC.2.4 for clarity. Also in FDP_ETC.2.4 “the following rules” was changed to “the following additional rules” to improve legibility and does not affect the meaning of the functional requirement.

6.4.3.4 FDP_IFF.1 (1) Simple Security Attributes

In FDP_IFF.1.3 (1) “enforce the” was changed to “enforce the following additional rules” and in FDP_IFF.1.4 (1) “provide the following” was changed to “provide the following additional capabilities”. Both refinements were made to improve legibility and do not affect the meaning of the functional requirement.

6.4.3.5 FDP_IFF.1 (2) Simple Security Attributes

In FDP_IFF.1.3 (2) “enforce the” was changed to “enforce the following additional rules” and in FDP_IFF.1.4 (2) “provide the following” was changed to “provide the following additional capabilities”. Both refinements were made to improve legibility and do not affect the meaning of the functional requirement.

6.4.3.6 FDP_IFF.1 (3) Simple Security Attributes

In FDP_IFF.1.3 (3) “enforce the” was changed to “enforce the following additional rules” and in FDP_IFF.1.4 (3) “provide the following” was changed to “provide the following additional capabilities”. Both refinements were made to improve legibility and do not affect the meaning of the functional requirement.

6.4.3.7 FDP_IFF.1 (4) Simple Security Attributes

In FDP_IFF.1.3 (4) “enforce the” was changed to “enforce the following additional rules” and in FDP_IFF.1.4 (4) “provide the following” was changed to “provide the following additional capabilities”. Both refinements were made to improve legibility and do not affect the meaning of the functional requirement.

6.4.3.8 FDP_IFF.1 (5) Simple Security Attributes

In FDP_IFF.1.3 (5) “enforce the” was changed to “enforce the following additional rules” and in FDP_IFF.1.4 (5) “provide the following” was changed to “provide the following additional capabilities”. Both refinements were made to improve legibility and do not affect the meaning of the functional requirement.

6.4.3.9 FDP_IFF.1 (6) Simple Security Attributes

In FDP_IFF.1.3 (6) “enforce the” was changed to “enforce the following additional rules” and in FDP_IFF.1.4 (6) “provide the following” was changed to “provide the following additional capabilities”. Both refinements were made to improve legibility and do not affect the meaning of the functional requirement.

6.4.3.10 FDP_IFF.1 (7) Simple Security Attributes

In FDP_IFF.1.3 (7) “enforce the” was changed to “enforce the following additional rules” and in FDP_IFF.1.4 (7) “provide the following” was changed to “provide the following additional capabilities”. Both refinements were made to improve legibility and do not affect the meaning of the functional requirement.

6.4.3.11 FDP_IFF.1 (8) Simple Security Attributes

In FDP_IFF.1.3 (8) “enforce the” was changed to “enforce the following additional rules” and in FDP_IFF.1.4 (8) “provide the following” was changed to “provide the following additional capabilities”. Both refinements were made to improve legibility and do not affect the meaning of the functional requirement.

6.4.3.12 FDP_ITC.2 Import of User Data with Security Attributes

The GME_SFP is only applicable for communication between the TOE and the BlackBerry Infrastructure, thus “outside the TOE” was changed to “to the BlackBerry Infrastructure” in FDP_ITC.2.1 and FDP_ITC.2.5 for clarity. Also in FDP_ITC.2.5 “the following rules” was changed to “the following additional rules” to improve legibility and does not affect the meaning of the functional requirement.

6.4.3.13 FPT_TDC.1 Inter-TSF Basic TSF Data Consistency

The GME specification is only used for communication between the TSF and the BlackBerry Infrastructure, thus in FPT_TDC.1.1 and FPT_TDC.1.2 “another trusted IT product” was changed to “the BlackBerry Infrastructure” for clarity.

6.4.3.14 FTP_ITC.1 Inter-TSF Trusted Channel

The requirement is placed on communication between the TSF and the BlackBerry Infrastructure, thus “another trusted IT product” was changed to “the BlackBerry Infrastructure” in FPT_TDC.1.1 and FPT_TDC.1.2 for clarity.

6.4.4 Selection of Security Assurance Requirements

The selection of EAL 4 assurance package is commensurate with the environment in which the TOE executes, and the augmentation of ALC_FLR.1 is appropriate to provide assurance to customers that security flaws are tracked and corrected.

The selected security assurance requirements are also applicable and appropriate for the explicitly stated security functional requirements, as the associated documentary evidence provide sufficient assurance for EAL 4, augmented by ALC_FLR.1.

The following table demonstrates that all SAR dependencies are satisfied.

Table 6. SAR Dependencies

Requirement	Dependencies	Satisfied By
ASE_CCL.1	ASE_ECD.1	ASE_ECD.1
	ASE_INT.1	ASE_INT.1
	ASE_REQ.1	ASE_REQ.1
ASE_ECD.1	None	–
ASE_INT.1	None	–
ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1
ASE_REQ.2	ASE_ECD.1	ASE_ECD.1
	ASE_OBJ.2	ASE_OBJ.2
ASE_SPD.1	None	–
ASE_TSS.1	ADV_FSP.1	ADV_FSP.1
	ASE_ECD.1	ASE_ECD.1
	ASE_OBJ.2	ASE_OBJ.2
ADV_FSP.4	ADV_TDS.1	ADV_TDS.1
ADV_TDS.3	ADV_FSP.4	ADV_FSP.4
ADV_ARC.1	ADV_FSP.1	ADV_FSP.1
	ADV_TDS.1	ADV_TDS.1
ADV_IMP.1	ADV_TDS.3	ADV_TDS.3
	ALC_TAT.1	ALC_TAT.1
AGD_OPE.1	ADV_FSP.1	ADV_FSP.1
AGD_PRE.1	None	–
ALC_FLR.1	None	–
ALC_CMC.4	ALC_CMS.1	ALC_CMS.1
	ALC_DVS.1	ALC_DVS.1
	ALC_LCD.1	ALC_LCD.1
ALC_CMS.4	None	–
ALC_DEL.1	None	–
ALC_DVS.1	None	–

Requirement	Dependencies	Satisfied By
ALC_LCD.1	None	–
ALC_TAT.1	ADV_IMP.1	ADV_IMP.1
ATE_COV.2	ADV_FSP.2	ADV_FSP.1
	ATE_FUN.1	ATE_FUN.1
ATE_FUN.1	ATE_COV.1	ATE_COV.1
ATE_IND.2	ADV_FSP.2	ADV_FSP.2
	AGD_OPE.1	AGD_OPE.1
	AGD_PRE.1	AGD_PRE.1
	ATE_FUN.1	ATE_FUN.1
	ATE_COV.1	ATE_COV.1
ATE_DPT.1	ADV_TDS.3	ADV_TDS.3
	ADV_ARC.1	ADV_ARC.1
	ATE_FUN.1	ATE_FUN.1
AVA_VAN.3	ADV_FSP.2	ADV_FSP.2
	ADV_TDS.3	ADV_TDS.3
	ADV_IMP.1	ADV_IMP.1
	ADV_ARC.1	ADV_ARC.1
	AGD_OPE.1	AGD_OPE.1
	AGD_PRE.1	AGD_PRE.1

6.4.5 Refinements of Security Assurance Requirements on the TOE

Refinement operations are not performed on any of the SARs on the TOE.

7 TOE Summary Specification

7.1 Security Functions

The TOE implements the following security functions:

7.1.1 F.GME Gateway Message Envelope Protocol

The TOE implements the RIM-proprietary GME protocol to wirelessly communicate with the BlackBerry Infrastructure for routing data to a BlackBerry Enterprise Server or another BlackBerry device. When sending data to either type of destination, the TOE sends its PIN, the data, and the identifier of the destination entity to the BlackBerry Infrastructure. The BlackBerry Infrastructure, in turn, routes the provided information. The identifier for a BlackBerry Enterprise Server is its UID, and the identifier for a BlackBerry device is its PIN. Receiving data from a BlackBerry Enterprise Server or another BlackBerry device is also accomplished through communication with the BlackBerry Infrastructure using the GME protocol. The communication between the TOE and the BlackBerry Infrastructure is initiated by the TOE when sending information from the TOE and is initiated by the BlackBerry Infrastructure when receiving information to the TOE. The TOE contains a GME service book that contains the UID of the BlackBerry Enterprise Server that administers the TOE.

The ability to send data to another BlackBerry device (i.e. send a PIN message) is determined by the value of the **Allow Peer-to-Peer Messages** IT policy rule, as described in F.ITPolicy.

7.1.2 F.Transport Secure Data Transport

Data transmitted between the TOE and a BlackBerry Enterprise Server or another BlackBerry device, as described in F.GME, is encrypted using AES-256 or Triple DES. If the destination is a BlackBerry Enterprise Server then the encryption algorithm is AES. If the destination is another BlackBerry device then the Triple DES algorithm is used.

When sending data, the TOE splits the data into 2 KB datagrams and encrypts each datagram with a unique session key created using the FIPS 186-2 PRNG. If the destination is a BlackBerry Enterprise Server then the session key is encrypted with the master encryption key, and if the destination is another BlackBerry device then the session key is encrypted with the peer-to-peer encryption key. The TOE then transmits the encrypted datagram and encrypted session key to the BlackBerry Infrastructure for routing, as described in F.GME.

When receiving data from a BlackBerry Enterprise Server or another BlackBerry device, the TOE selects the master encryption key or peer-to-peer encryption key accordingly and decrypts the encrypted session key. The session key is then used to decrypt the encrypted datagram.

7.1.3 F.Kernel BlackBerry Cryptographic Kernel

The BlackBerry Cryptographic Kernel is the cryptographic module responsible for supporting secure data transport from the TOE, wireless generation of a new master encryption key through key agreement, and the content protection feature. It implements the following cryptographic algorithms:

- AES-256 (CBC mode of operation)
- Triple DES (CBC mode of operation)
- SHA-1, -256, and -512
- HMAC SHA-1, -256, and -512
- RSA PKCS#1 (1024 bit, signature verification only)
- FIPS 186-2 Appendix 3.1 PRNG

- ECDSA (571 bit, signature verification only)
- EC Diffie-Hellman
- EC MQV

Version 3.8.5.85 of the BlackBerry Cryptographic Kernel is included in Device Software Version 5.0.0 and has been awarded FIPS 140-2 validation certificate no.1252.

7.1.4 F.Wireless Wireless Communication

The TOE provides the following wireless capabilities:

- Email messaging – The TOE allows the device user to send and receive email messages using their enterprise email account. Email messaging is accomplished by communication between the TOE and a BlackBerry Enterprise Server, as described in F.Transport.
- PIM synchronisation – The TOE bi-directionally synchronises PIM data with the user's enterprise email account via communication with the BlackBerry Enterprise Server, as described in F.Transport.
- PIN messaging – The TOE allows the device user to send and receive PIN messages to and from other BlackBerry devices, as described in F.Transport.
- Cellular phone – The TOE allows the device user to send and receive cellular phone communication.
- SMS messaging – The TOE allows the device user to send and receive SMS messages.
- MMS messaging – The TOE allows the device user to send and receive MMS messages.
- Bluetooth communication – The TOE supports the Hands Free and Headset Bluetooth profiles that allow the TOE to communicate with other Bluetooth devices.
- WiFi communication – The TOE supports a type of local area network that uses high-frequency radio waves rather than wires to communicate between nodes.
- GPS communication – The TOE supports location-based applications and location-based services.

The TOE provides remote management capabilities of its wireless communication functionality through the use of IT policy, as described in F.ITPolicy.

7.1.5 F.Administration Local Administration

The TOE provides management capabilities that allow the device user to perform the following administrative functions:

- Lock device
- Modify device password
- Perform security wipe of the device
- Cooperatively generate new master encryption key with BlackBerry Enterprise Server

The TOE also allows the device user to perform the following administrative functions, dependent upon the IT policy configuration per F.ITPolicy:

- Modify security timeout
- Enable and disable device locking when holstered
- Enable and disable content protection on the TOE
- Enable and disable Bluetooth functionality

- Enable and disable WiFi functionality
- Modify allowed and disallowed S/MIME content ciphers

7.1.6 F.ITCommand Wireless IT Commands

The TOE is able to execute IT commands issued by the BlackBerry Enterprise Server administrator. An IT command is only executed if the TOE determines that the source BlackBerry Enterprise Server is authorised to issue the command. The TOE determines proper authorisation by verifying that the timestamp of the IT command is not older than the timestamp of the most recently executed IT command and that the UID of the source BlackBerry Enterprise Server matches the UID of the BlackBerry Enterprise Server that issued the current IT policy configuration. Depending on the IT command type, data may be included to support the execution of the IT command.

The TOE is able to execute the IT commands described in the following table.

Table 7. IT Commands

IT Command	Includes IT Command Data?	Description
Erase Data and Disable Handheld	No	Erases all user data on the device. The device is returned to its factory default settings and is no longer integrated with the email account of the device user.
Set Password and Lock	Yes	Sets the device password to the password specified in the IT command data and locks the device.
Set IT Policy	Yes	Sets the current IT policy configuration enforced by the TOE to the IT policy configuration specified in the IT command data. See F.ITPolicy for more information.

7.1.7 F.ITPolicy Wireless IT Policy

The TOE is able to enforce the IT policy configuration specified and issued by the BlackBerry Enterprise Server administrator. An IT policy configuration is only enforced if the TOE determines the source BlackBerry Enterprise Server is authorised to specify the configuration. The TOE determines proper authorisation by verifying that the ECDSA signature of the new IT policy configuration and the included ECDSA public key verifies successfully using the ECDSA public key included with the current IT policy configuration.[6]

If the TOE determines an IT policy configuration is to be enforced then it replaces the current IT policy configuration with the new configuration. If there is no current IT policy configuration then the new configuration is automatically enforced.

The TOE is able to enforce an IT policy configuration that consists of the IT policy rules specified in the following table, which is a subset of the entire set of IT policy rules supported by the TOE. Refer to Baseline Configuration on page 69 for configuration information on the listed IT policy rules.

Table 8. IT Policy Rules

IT Policy Rule	Description
Allow Browser	Controls whether the user can use the default browser included on the device.

[6] Note that the conditions specified in F.ITCommand must be satisfied before the TOE will execute the **Set IT Policy** IT command.

IT Policy Rule	Description
Allow External Connections	Controls whether third-party applications on the device can initiate external connections (e.g., to WAP or other public gateway).
Allow Internal Connections	Controls whether third-party applications on the device can initiate internal connections (e.g., to the Mobile Data Service).
Allow Peer-to-Peer Messages	Specifies whether device users can send PIN messages. This rule does not prevent device users from receiving PIN messages.
Allow Phone	Specifies whether device users can access phone capabilities. This rule does not prevent device users from making emergency phone calls.
Allow SMS	Specifies whether device users can send and receive SMS messages.
Allow Third Party Apps to Use Serial Port	Specifies whether third-party applications can use the USB port on the device.
Content Protection Strength	Forces the use of the content protection feature and specifies the strength of the ECDH key pair used to generate an AES-256 key while the device is locked. Null – Content protection is not forcibly enabled 0 – 160 bits 1 – 256 bits 2 – 521 bits
Disable 3DES Transport Crypto	Forces the device to encrypt and decrypt packets to and from the BlackBerry Enterprise Server that sent the IT policy using AES instead of Triple DES.
Disable All Wireless Sync	Disables wireless synchronisation of PIM data.
Disable Bluetooth	Disables all Bluetooth support.
Disable External Memory	Specifies whether to prevent the expandable memory (microSD) feature from working on supported BlackBerry devices.
Disable GPS	Specifies whether the GPS functionality on the BlackBerry device is turned on.
Disable JavaScript in Browser	Specifies whether to prevent JavaScript execution in the BlackBerry Browser.
Disable MMS	Specifies whether to prevent the BlackBerry device user from using Multimedia Messaging Service (MMS) functionality on the BlackBerry device.
Disable Photo Camera	Specifies whether the ability to take still pictures with the camera is turned off on the BlackBerry device.
Disable USB Mass Storage	Specifies whether to prevent the USB Mass Storage feature from working on supported BlackBerry devices.
Disable Video Camera	Specifies whether the ability to record video with the camera is turned off on the BlackBerry device.\n\nSet this rule to True to turn off the video camera feature.
Disable Voice Note Recording	Specifies whether the voice note recording feature on the BlackBerry device is turned on.
Disable WLAN	Disables use of WLAN on the device.
Disallow Third Party Application Downloads	Specifies whether third-party applications may be downloaded and installed on the device.
Enable Long Term Timeout	Controls whether the device locks after a predefined period of time, regardless of user activity.
Force Lock When Holstered	Specifies whether the device is locked when placed in the holster.

IT Policy Rule	Description
Maximum Password Age	Specifies the number of days until a device password expires and the user is prompted to provide a new password. 0 – The password never expires. 1-65535 – The password expires after the specified number of days.
Maximum Password History	Specifies the maximum number of previous device passwords against which new passwords can be checked to prevent reuse of the old passwords. 0 – The password is not checked against previous passwords. 1-15 – The password is checked against the specified number of previous passwords.
Maximum Security Timeout	Specifies the maximum time, in minutes, allowed before a device security timeout occurs. The device user can select any timeout value less than the maximum value.
Minimum Password Length	Specifies the minimum allowable length, in characters, of the device password.
Password Pattern Checks	Creates a pattern check on the device password. 0 – No restrictions. 1 – The password must contain at least one alpha and one numeric character. 2 – The password must contain at least one alpha, one numeric, and one special character. 3 – The password must contain at least one uppercase alpha, one lowercase alpha, one numeric, and one special character.
Password Required	Specifies whether the use of a device password is required.
Periodic Challenge Time	Specifies the interval, in minutes, after which the user is prompted to enter a password, regardless of user activity.
Set Maximum Password Attempts	Specifies the number of unsuccessful authentication attempts (i.e. the number of incorrect passwords entered) allowed on the device before the device data is erased and the device disabled.
Set Password Timeout	Specifies the amount of time, in minutes, before the security timeout occurs on the device.
S/MIME Allowed Content Ciphers	Specifies the content ciphers that the BlackBerry device can use to encrypt S/MIME messages.
Suppress Password Echo	Disables the echoing (printing to the screen) of characters typed into the device password screen[7].
User Can Change Timeout	Specifies whether the device user can change the specified security timeout.

7.1.8 F.Authentication Authentication

The TOE provides a password-based authentication mechanism with the following functionality that can be configured per F.Administration or F.ITPolicy:

- Limited feedback during authentication (an asterisk is displayed for each character typed)
- Authentication failure handling (a security wipe of device executed after multiple failed authentication attempts)
- Password pattern checking
- Time-based password expiration, requiring the user to change the password
- Session locking, requiring user re-authentication, based on the following events:

[7] BlackBerry devices that use SureType® technology, briefly display feedback to the user before masking password characters with an asterisk

- A time interval of inactivity elapsing
- User invocation
- TOE placed in holster
- **Set Password and Lock** IT command received per F.ITCommand

The following actions may be performed by the TOE prior to user authentication:

- Receive email, PIN, SMS and MMS messages
- Receive calendar appointments
- Synchronise PIM data
- Receive cellular phone communication
- Make emergency cellular phone communication (e.g. 911)

7.1.9 F.Time Time

The TOE provides reliable date and time information.

7.1.10 F.Applications Third-Party Applications

The TOE provides the ability to download, install, and execute third-party applications subject to the restrictions specified by the BlackBerry Enterprise Server administrator per F.ITPolicy.

7.1.11 F.Content Protection of Stored Content

The TOE provides the content protection and security wipe features to protect stored user data from unauthorised disclosure. The content protection feature encrypts stored data using AES-256. When enabled, the content protection feature encrypts the following stored user data:

- Email – Subject, email addresses, message body, attachments
- Calendar – Subject, location, organiser, attendees, notes included in the appointment or meeting request
- MemoPad – Title, information in the note body
- Tasks – Subject, information in the task body
- Contacts – All information except for title and category
- Auto Text – All entries that the original text is replaced with
- BlackBerry Browser – Content that is pushed to the TOE, websites that are saved on the TOE, browser cache

If the content protection feature in enabled and the device receives new user data while locked, ECDH key agreement is used to generate a temporary AES-256 key to encrypt the new user data. The content protection feature may be enabled and configured by the user or BlackBerry Enterprise Server administrator per F.Administration and F.ITPolicy, respectively.

The security wipe feature programmatically erases all stored user data and can be invoked automatically or manually. If the TOE is configured to require user authentication then the feature is automatically invoked when the maximum number of unsuccessful authentication attempts is reached. The feature can also be invoked manually by the user or BlackBerry Enterprise Server administrator per F.Administration and F.ITCommand, respectively.

7.1.12 F.S/MIME S/MIME

The TOE provides added confidentiality and further protects the integrity and privacy of messages as well as additional layer of security and end-to-end authentication.

The TOE is designed to support using a strong algorithm for S/MIME encryption. When the user turns on S/MIME encryption on the BlackBerry Enterprise Server, the S/MIME Allowed Content Ciphers IT policy rule default setting specifies that the BlackBerry device can use any of the supported algorithms (other than the two weakest RC2 algorithms, RC2 (64-bit) and RC2 (40-bit)) to encrypt S/MIME messages.

User can set the S/MIME Allowed Content Ciphers IT policy rule to encrypt S/MIME messages using any of AES (256-bit), AES (192-bit), AES (128-bit), Triple DES.

If the BlackBerry device has previously received a message from the intended recipient, the BlackBerry device is designed to recall which content ciphers the recipient can support, and use one of those ciphers. The BlackBerry device encrypts the message using Triple DES by default if it does not know the decryption capabilities of the recipient.

7.1.13 F.SWConfiguration Software Configuration

The TOE provides the ability to control access of third-party applications to TOE resources and user data subject to the restrictions specified by the BlackBerry Enterprise Server administrator. The user can make application access control configuration more restrictive by changing application permissions on the TOE.

The TOE is able to enforce a software configuration that consists of the software configuration policy rules specified in the following table, which is a subset of the entire set of the software configuration policy rules supported by the TOE.

Table 9. Software Configuration Rules

Software Configuration Rule	Description
Disposition	Specify whether the application is optional, required, or not allowed on the BlackBerry device. You can use this application control policy rule to require that the BlackBerry device download a specific application or prevent the BlackBerry device from downloading an unspecified or untrusted application.
Interprocess Communication	Specify whether or not the application can perform interprocess communication operations. You can use this application control policy rule to prevent two or more applications from sharing data and to prevent one application from using the connection permissions of another application.
Internal Network Connections	Specify whether or not the application can make internal corporate network connections. You can use this application control policy rule to allow or prevent the application from sending or receiving data on the BlackBerry device using an internal protocol (for example, using the connection service) or to require that the user respond to a prompt on the BlackBerry device to allow internal connections through the BlackBerry device firewall.
External Network Connections	Specify whether or not the application can make external network connections. You can use this application control policy rule to allow or prevent the application from sending or receiving data on the BlackBerry device using an external protocol (for example, using a WAP gateway, public BlackBerry MDS Services, or TCP), or to require that the user respond to a prompt on their BlackBerry device to allow external connections through the BlackBerry device firewall.
Local Connections	Specify whether or not the application can make local network connections (for example, connections to the BlackBerry device using a USB or serial port).
Phone Access	Specify whether or not the application can make phone calls and access phone logs on the BlackBerry device. You can use this application control policy rule to allow or prevent the application from making calls on the BlackBerry device or to require that the user respond to a prompt on the BlackBerry device to allow the application to make a phone call.
Message Access	Specify whether or not the application can send and receive messages on the BlackBerry device using the email API.

Software Configuration Rule	Description
PIM Data Access	Specify whether or not the application can access the BlackBerry device PIM APIs, which control access to the user's personal information on the BlackBerry device, including the address book. **Note**: Allowing the application to access PIM data APIs and use internal and external network connection protocols creates an opportunity for an application to send all of the user's personal data from their BlackBerry device.
Browser Filters	Specify whether or not the application can access browser filter APIs to register a browser filter with the browser on the BlackBerry device. You can use this application control policy rule to allow third-party Java applications to apply custom browser filters to web page content on the BlackBerry device.
Event Injection	Specify whether or not the application can inject synthetic input events, such as pressing keys and performing trackwheel actions, on the BlackBerry device.
Bluetooth Serial Profile	Specify whether or not the application can access the Bluetooth® Serial Port Profile (SPP) API. **Note**: If you set the Disable Serial Port Profile IT policy rule to True, the Bluetooth enabled BlackBerry device cannot use the Bluetooth SPP to establish a serial connection to a Bluetooth enabled device.
BlackBerry Device Keystore	Specify whether or not the application can access the BlackBerry device key store APIs. If you set the Minimal Signing Key Store Security Level and the Minimal Encryption Key Store Security Level IT policy rules to high, the BlackBerry device prompts the user for the BlackBerry device key store password each time an application tries to access the user's private key on the BlackBerry device, and the BlackBerry device does not use this application policy control rule.
BlackBerry Device Keystore Medium Security	Specify whether or not the application can access key store items at the medium security level (the default level), which requires that the BlackBerry device prompt the user for the BlackBerry device key store password when an application tries to access the user's private key for the first time or when the private key password timeout expires. If you set the Minimal Signing Key Store Security Level and the Minimal Encryption Key Store Security Level IT policy rules to high, the BlackBerry device prompts the user for the BlackBerry device key store password each time an application tries to access their private key, and this application policy control rule is not recognized.
Device GPS	Specify whether or not the application can access the BlackBerry device Global Positioning System (GPS) APIs. You can use this application control policy rule to allow or prevent the application from accessing the GPS APIs on the BlackBerry device or to require that the user respond to a prompt on the BlackBerry device to allow access to the GPS APIs.
User Authenticator API	Specify whether or not the BlackBerry device allows an application to access the user authenticator framework API. The user authenticator framework allows the registration of drivers (currently smart card drivers only) that provide two-factor authentication to unlock the BlackBerry device. This application control policy rule applies to the BlackBerry Device Software and third-party Java applications.

7.1.14 F.Multimedia Multimedia Applications

The TOE provides multimedia applications, including photo camera, video camera, and voice note recording, subject to the restrictions specified by the BlackBerry Enterprise Server administrator per F.ITPolicy.

7.1.15 F.FileEncryption File Encryption

The TOE provides encryption of multimedia data stored on an external memory device using AES-256.

7.2 Assurance Measures

There exists TOE design documentation that consists of a functional specification, complete interface specification, description of the basic modular design of the TOE, and a subset of the implementation.

7.2.1 A.Configuration Configuration Management

There exists configuration management documentation that lists, uniquely identifies, and describes the configuration items that comprise the TOE. The configuration management system used to manage the TOE uniquely identifies all configuration items.

7.2.2 A.Delivery Delivery Procedures

There exists TOE delivery documentation that describes the procedures used to securely deliver the TOE.

7.2.3 A.Design Design Documentation

There exists TOE design documentation that consists of a functional specification, complete interface specification, description of the basic modular design of the TOE, and a subset of the implementation.

7.2.4 A.Guidance Guidance Documentation

The TOE includes guidance documentation that consists of a User Guide.

7.2.5 A.Remediation Flaw Remediation

There exists TOE flaw remediation documentation that describes the procedures used to track reported TOE security flaws.

7.2.6 A.Testing Developer Testing

Developer testing of the TOE has been performed and there exists testing documentation that consists of functional test plans, procedures, and results and evidence of coverage and depth of the TOE security functions.

7.2.7 A.Evaluator Evaluator Testing

The TOE has been provided to the evaluation facility for independent testing.

7.2.8 A.SecurityTarget Security Target

There exists a Security Target document that describes the TOE.

7.3 TOE Security Specification

7.3.1 TOE Security Functions

The following table maps the TOE security functions to the SFRs.

Table 10. Mapping of TOE Security Functions to SFRs

	F.GME	F.Transport	F.Kernel	F.Wireless	F.Administration	F.ITCommand	F.ITPolicy	F.Authentication	F.Time	F.Applications	F.Content	F.S/MIME	F.SWConfiguration	F.Multimedia	F.FileEncryption
FCS_VAL_EXP.1			X												
FCS_CKM.1 (1)			X												
FCS_CKM.1 (2)			X												
FCS_CKM.4			X												
FCS_COP.1			X									X			X
FDP_ACC.1 (1)							X								
FDP_ACF.1 (1)							X								
FDP_ACC.1 (2)					X										
FDP_ACF.1 (2)					X										
FDP_ACC.1 (3)													X		
FDP_ACF.1 (3)													X		
FDP_ETC.2	X														
FDP_IFC.1 (1)	X	X													
FDP_IFF.1 (1)	X	X													
FDP_IFC.1 (2)						X									
FDP_IFF.1 (2)						X									
FDP_IFC.1 (3)				X											
FDP_IFF.1 (3)				X											
FDP_IFC.1 (4)										X					
FDP_IFF.1 (4)										X					
FDP_IFC.1 (5)										X					
FDP_IFF.1 (5)										X					
FDP_IFC.1 (6)				X											
FDP_IFF.1 (6)				X											
FDP_IFC.1 (7)				X											
FDP_IFF.1 (7)				X											
FDP_IFC.1 (8)														X	
FDP_IFF.1 (8)														X	
FDP_ITC.2	X														
FDP_SDP_EXP.1											X				
FDP_SDP_EXP.2											X				
FIA_AFL.1							X	X							
FIA_SOS.1							X	X							
FIA_UAU.1					X		X	X							

	F.GME	F.Transport	F.Kernel	F.Wireless	F.Administration	F.ITCommand	F.ITPolicy	F.Authentication	F.Time	F.Applications	F.Content	F.S/MIME	F.SWConfiguration	F.Multimedia	F.FileEncryption
FIA_UAU.7							X	X							
FIA_UID.1					X		X	X							
FMT_MSA.1 (1)						X	X								
FMT_MSA.1 (2)						X	X								
FMT_MSA.1 (3)						X	X								
FMT_MSA.1 (4)							X								
FMT_MSA.2			X												
FMT_MSA.3 (1)						X	X								
FMT_MSA.3 (2)							X								
FMT_MSA.3 (3)	X						X								
FMT_MSA.3 (4)						X	X								
FMT_MSA.3 (5)							X								
FMT_MSA.3 (6)							X								
FMT_SAE.1							X	X							
FMT_SMF.1					X	X	X								
FPT_STM.1									X						
FPT_TDC.1	X														
FTA_SSL.1							X	X							
FTA_SSL.2								X							
FTA_SSL_EXP.4					X	X	X	X							
FTP_ITC.1	X														

7.3.1.1 FCS_VAL_EXP.1, Cryptographic module validation

The cryptographic module embedded in the TOE is validated to meet the requirements of FIPS 140-2 (F.Kernel).

7.3.1.2 FCS_CKM.1, Cryptographic key generation (1)

The cryptographic module embedded in the TOE is validated to FIPS 140-2 and generates keys using the FIPS 186-2 PRNG (F.Kernel).

7.3.1.3 FCS_CKM.1, Cryptographic key generation (2)

The cryptographic module embedded in the TOE is validated to FIPS 140-2 and generates keys using ECDH and ECMQV key agreement (F.Kernel).

7.3.1.4 FCS_CKM.4, Cryptographic key destruction

The cryptographic module embedded in the TOE is validated to FIPS 140-2 and destroys keys according to the FIPS 140-2 key zeroization requirements (F.Kernel).

7.3.1.5 FCS_COP.1, Cryptographic operation (1)

The cryptographic module embedded in the TOE is validated to FIPS 140-2 and provides the required cryptographic functionality (F.Kernel).

The TOE provides S/MIME messaging functionality (F.S/MIME).

The TOE provides file encryption on an external memory device (F.FileEncryption).

7.3.1.6 FDP_ACC.1, Subset access control (1)

The TOE accepts and enforces valid IT policy configurations received from the BlackBerry Enterprise Server administrator (F.ITPolicy).

FDP_ACF.1, Security attribute based access control (1)

The TOE accepts and enforces valid IT policy configurations received from the BlackBerry Enterprise Server administrator (F.ITPolicy).

7.3.1.7 FDP_ACC.1, Subset access control (2)

The TOE user cannot override the IT policy configuration specified by the BlackBerry Enterprise Server administrator (F.Administration).

FDP_ACF.1, Security attribute based access control (2)

The TOE user cannot override the IT policy configuration specified by the BlackBerry Enterprise Server administrator (F.Administration).

7.3.1.8 FDP_ACC.1, Subset access control (3)

The TOE accepts and enforces valid software configurations received from the BlackBerry Enterprise Server administrator (F.SWConfiguration).

FDP_ACF.1, Security attribute based access control (3)

The TOE accepts and enforces valid software configurations received from the BlackBerry Enterprise Server administrator (F.SWConfiguration).

7.3.1.9 FDP_ACC.1, Subset access control (3)

The TOE user cannot override the software configuration specified by the BlackBerry Enterprise Server administrator (F.Administration).

FDP_ACF.1, Security attribute based access control (3)

The TOE user cannot override the software configuration specified by the BlackBerry Enterprise Server administrator (F.Administration).

7.3.1.10 FDP_ETC.2, Export of user data with security attributes

When sending data to the BlackBerry Infrastructure for routing to a BlackBerry Enterprise Server or another BlackBerry device, the GME protocol ensures that user data sent from the TOE is associated with the PIN of the TOE (F.GME).

7.3.1.11 FDP_IFC.1, Subset information flow control (1)

All communication between the TOE and a BlackBerry Enterprise Server or another BlackBerry device is routed by the BlackBerry Infrastructure, and the communication between the TOE and the BlackBerry Infrastructure follows the GME protocol (F.GME). All data transferred between the TOE and a BlackBerry Enterprise Server or another BlackBerry device is protected (F.Transport).

7.3.1.12 FDP_IFF.1, Simple security attributes (1)

All communication between the TOE and a BlackBerry Enterprise Server or another BlackBerry device is routed by the BlackBerry Infrastructure, and the communication between the TOE and the BlackBerry Infrastructure follows the GME protocol (F.GME). All data transferred between the TOE and a BlackBerry Enterprise Server or another BlackBerry device is protected (F.Transport).

7.3.1.13 FDP_IFC.1, Subset information flow control (2)

The TOE executes valid IT commands received from the BlackBerry Enterprise Server administrator (F.ITCommand).

7.3.1.14 FDP_IFF.1, Simple security attributes (2)

The TOE executes valid IT commands received from the BlackBerry Enterprise Server administrator (F.ITCommand).

7.3.1.15 FDP_IFC.1, Subset information flow control (3)

The TOE synchronises PIM data with the user's enterprise email account (F.Wireless).

7.3.1.16 FDP_IFF.1, Simple security attributes (3)

The TOE synchronises PIM data with the user's enterprise email account (F.Wireless).

7.3.1.17 FDP_IFC.1, Subset information flow control (4)

The TOE provides the ability to download third-party applications (F.Applications).

7.3.1.18 FDP_IFF.1, Simple security attributes (4)

The TOE provides the ability to download third-party applications (F.Applications).

7.3.1.19 FDP_IFC.1, Subset information flow control (5)

The TOE provides internal and external network access to third-party applications (F.Applications).

7.3.1.20 FDP_IFF.1, Simple security attributes (5)

The TOE provides internal and external network access to third-party applications (F.Applications).

7.3.1.21 FDP_IFC.1, Subset information flow control (6)

The TOE provides cellular phone communication functionality (F.Wireless).

7.3.1.22 FDP_IFF.1, Simple security attributes (6)

The TOE provides cellular phone communication functionality (F.Wireless).

7.3.1.23 FDP_IFC.1, Subset information flow control (7)

The TOE provides Bluetooth, WiFi and GPS communication functionality (F.Wireless).

7.3.1.24 FDP_IFF.1, Simple security attributes (7)

The TOE provides Bluetooth, WiFi and GPS communication functionality (F.Wireless).

7.3.1.25 FDP_IFC.1, Subset information flow control (8)

The TOE provides the ability to control multimedia applications (F.Multimedia).

7.3.1.26 FDP_IFF.1, Simple security attributes (8)

The TOE provides the ability to control multimedia applications (F.Multimedia).

7.3.1.27 FDP_ITC.2, Import of user data with security attributes

When receiving data from a BlackBerry Enterprise Server or another BlackBerry device, the GME protocol ensures that user data sent to the TOE from the BlackBerry Infrastructure is associated with the PIN of the device (F.GME).

7.3.1.28 FDP_SDP_EXP.1, Stored data non-disclosure

The TOE is capable of cryptographically protecting stored user data (F.Content).

7.3.1.29 FDP_SDP_EXP.2, Stored data deletion

The TOE is capable of protecting stored user data from unauthorised disclosure by programmatically erasing all user data (F.Content).

7.3.1.30 FIA_AFL.1, Authentication failure handling

The TOE can be configured to perform a security wipe of all user data after a configurable number of failed authentication attempts (F.ITPolicy, F.Authentication).

7.3.1.31 FIA_SOS.1, Verification of secrets

The TOE can be configured to enforce quality metrics on the TOE password (F.ITPolicy, F.Authentication).

7.3.1.32 FIA_UAU.1, Timing of authentication

The TOE can be configured to require password-based user authentication (F.Administration, F.ITPolicy, F.Authentication).

7.3.1.33 FIA_UAU.7, Protected authentication feedback

The TOE can be configured to display an asterisk for each character typed during the authentication process (F.ITPolicy, F.Authentication).

7.3.1.34 FIA_UID.1, Timing of identification

The TOE can be configured to require password-based user authentication (F.Administration, F.ITPolicy, F.Authentication).

7.3.1.35 FMT_MSA.1, Management of security attributes (1)

The TOE executes IT commands and enforces IT policy configurations issued by the BlackBerry Enterprise Server administrator (F.ITCommand, F.ITPolicy).

7.3.1.36 FMT_MSA.1, Management of security attributes (2)

The TOE executes IT commands and enforces IT policy configurations issued by the BlackBerry Enterprise Server administrator (F.ITCommand, F.ITPolicy).

7.3.1.37 FMT_MSA.1, Management of security attributes (3)

The TOE executes IT commands and enforces IT policy configurations issued by the BlackBerry Enterprise Server administrator (F.ITCommand, F.ITPolicy).

7.3.1.38 FMT_MSA.1, Management of security attributes (4)

The TOE enforces software configuration issued by the BlackBerry Enterprise Server administrator (F.ITPolicy).

7.3.1.39 FMT_MSA.2, Secure security attributes

The BlackBerry Cryptographic Kernel ensures that only secure cryptographic values are accepted and utilised, per the requirements of FIPS 140-2 (F.Kernel).

7.3.1.40 FMT_MSA.3, Static attribute initialisation (1)

The IT command type and data and UID of source BlackBerry Enterprise Server are specified by the BlackBerry Enterprise Server administrator (F.ITCommand, F.ITPolicy).

7.3.1.41 FMT_MSA.3, Static attribute initialisation (2)

The IT policy configuration enforced by the TOE, which consequently limits the administrative abilities of the TOE user, is specified by the BlackBerry Enterprise Server administrator (F.ITPolicy).

7.3.1.42 FMT_MSA.3, Static attribute initialisation (3)

The IT policy configuration enforced by the TOE is specified by the BlackBerry Enterprise Server administrator (F.ITPolicy). The GME service book of the TOE is issued by the BlackBerry Enterprise Server administrator (F.GME).

7.3.1.43 FMT_MSA.3, Static attribute initialisation (4)

The IT command type and data and UID of source BlackBerry Enterprise Server are specified by the BlackBerry Enterprise Server administrator (F.ITCommand, F.ITPolicy).

7.3.1.44 FMT_MSA.3, Static attribute initialisation (5)

The IT policy configuration enforced by the TOE is specified by the BlackBerry Enterprise Server administrator (F.ITPolicy).

7.3.1.45 FMT_MSA.3, Static attribute initialisation (6)

The software configuration enforced by the TOE, which consequently limits the administrative abilities of the TOE user, is specified by the BlackBerry Enterprise Server administrator (F.ITPolicy).

7.3.1.46 FMT_SAE.1, Time-limited authorisation

The BlackBerry Enterprise Server administrator can specify an expiration time for the TOE password, which when elapsed forces the user to change the password (F.ITPolicy, F.Authentication).

7.3.1.47 FMT_SMF.1, Specification of management functions

The TOE provides management capabilities to the local user (F.Administration) and the BlackBerry Enterprise Server administrator (F.ITCommand, F.ITPolicy).

7.3.1.48 FPT_STM.1, Reliable time stamps

The TOE provides reliable date and time information (F.Time).

7.3.1.49 FPT_TDC.1, Inter-TSF basic TSF data consistency

The TOE communicates with the BlackBerry Infrastructure using the GME protocol (F.GME).

7.3.1.50 FTA_SSL.1, TSF-initiated session locking

The interactive session with the TOE locks after a specified time interval of inactivity configured by the BlackBerry Enterprise Server administrator (F.Authentication, F.ITPolicy).

7.3.1.51 FTA_SSL.2, User-initiated locking

The user can lock the interactive session with the TOE (F.Authentication).

7.3.1.52 FTA_SSL_EXP.4, Event-initiated session locking

The BlackBerry Enterprise Server administrator can lock the user's interactive session with the TOE by issuing the **Set Password and Lock** IT command (F.Authentication, F.ITCommand). The interactive session with the TOE can be configured to lock after the TOE is placed in its holster (F.Administration, F.Authentication, F.ITPolicy).

7.3.1.53 FTP_ITC.1, Inter-TSF trusted channel

The GME protocol ensures a distinct communication channel between the TOE and the BlackBerry Infrastructure, where either entity can initiate communication (F.GME).

7.3.2 TOE Assurance Measures

The following table maps the TOE assurance measures to the SARs.

Table 11. Mapping of TOE Assurance Measures to SARs

	A.Configuration	A.Delivery	A.Design	A.Guidance	A.Remediation	A.Testing	A.Evaluator	A.Assessment	A.SecurityTarget
ASE_CCL.1									X
ASE_ECD.1									X
ASE_INT.1									X
ASE_OBJ.2									X
ASE_REQ.2									X
ASE_SPD.1									X

	A.Configuration	A.Delivery	A.Design	A.Guidance	A.Remediation	A.Testing	A.Evaluator	A.Assessment	A.SecurityTarget
ASE_TSS.1									X
ADV_FSP.4			X						
ADV_ARC.1			X						
ADV_TDS.3			X						
ADV_IMP.1			X						
AGD_OPE.1				X					
AGD_PRE.1				X					
ALC_CMC.4	X								
ALC_CMS.4	X								
ALC_DEL.1		X							
ALC_DVS.1	X								
ALC_LCD.1	X								
ALC_TAT.1	X								
ALC_FLR.1					X				
ATE_COV.2						X			
ATE_FUN.1						X			
ATE_IND.2							X		
ATE_DPT.1						X			
AVA_VAN.3								X	

7.3.2.1 ASE_CCL.1, Conformance claims

The Conformance claims section exists in the Security Target (A.SecurityTarget).

7.3.2.2 ASE_ECD.1, Extended components definition

The Extended components definition section exists in the Security Target (A.SecurityTarget).

7.3.2.3 ASE_INT.1, ST introduction

The ST introduction section exists in the Security Target (A.SecurityTarget).

7.3.2.4 ASE_OBJ.2, Security objectives

The Security objectives section exists in the Security Target (A.SecurityTarget).

7.3.2.5 ASE_REQ.2, Derived security requirements

The Derived security requirements section exists in the Security Target (A.SecurityTarget).

7.3.2.6 ASE_SPD.1, Security problem definition

The Security problem definition section exists in the Security Target (A.SecurityTarget).

7.3.2.7 ASE_TSS.1, TOE summary specification

The TOE summary specification section exists in the Security Target (A.SecurityTarget).

7.3.2.8 ADV_FSP.4, Complete functional specification

There exists design documentation (A.Design).

7.3.2.9 ADV_ARC.1, Security architecture description

There exists design documentation (A.Design).

7.3.2.10 ADV_TDS.3, Basic modular design

There exists design documentation (A.Design).

7.3.2.11 ADV_IMP.1, Implementation representation of the TSF

There exists design documentation (A.Design).

7.3.2.12 AGD_OPE.1, Operational user guidance

The TOE includes operational user guidance documentation (A.Guidance).

7.3.2.13 AGD_PRE.1, Preparative procedures

The TOE includes preparative procedures documentation (A.Guidance).

7.3.2.14 ALC_CMC.4, Production support, acceptance procedures and automation

There exists production support, acceptance procedures and automation documentation (A.Configuration)

7.3.2.15 ALC_CMS.4, Problem tracking CM coverage

There exists problem tracking CM coverage documentation (A.Configuration)

7.3.2.16 ALC_DEL.1, Delivery procedures

There exists delivery procedures documentation (A.Delivery)

7.3.2.17 ALC_DVS.1, Identification of security measures

There exists identification of security measures procedure documentation (A.Configuration)

7.3.2.18 ALC_LCD.1, Developer defined life-cycle model

There exists life-cycle model documentation (A.Configuration)

7.3.2.19 ALC_TAT.1, Well-defined development tools

There exists development tools documentation (A.Configuration)

7.3.2.20 ALC_FLR.1, Basic flaw remediation

There exists flaw remediation procedures documentation (A.Remediation).

7.3.2.21 ATE_COV.2, Analysis of coverage

Developer testing of the TOE has been performed and there exists testing documentation (A.Testing).

7.3.2.22 ATE_FUN.1, Functional testing

Developer testing of the TOE has been performed and there exists testing documentation, including evidence of testing coverage (A.Testing).

7.3.2.23 ATE_DPT.1, Testing: basic design

Developer testing of the TOE has been performed and there exists testing documentation, including evidence of depth of testing (A.Testing).

7.3.2.24 ATE_IND.2, Independent testing – sample

The TOE has been provided to the evaluation facility (A.Evaluator).

7.3.2.25 AVA_VAN.3, Focused vulnerability analysis

A vulnerability assessment of the TOE has been performed and documented (A.Assessment).

8 Baseline Configuration

8.1 Baseline IT Policy Configuration

The baseline IT policy configuration is the evaluated configuration of the TOE that provides the most flexibility to tailor the listed IT policy rules to comply with an enterprise security policy. The deployed configuration of the TOE shall be at least as restrictive as the baseline configuration. The following table identifies the valid range of values, default value, and baseline value for each IT policy rule specified F.ITPolicy. With the exception of the values marked with an asterisk ("*"), modifying the baseline values will result in a more restrictive configuration, and thus may be configured to comply with an enterprise security policy while maintaining an evaluated configuration.

Table 12. Baseline IT Policy Configuration

IT Policy Rule	Value		
	Range	Default	Baseline
Global Policy Group			
Allow Browser	{True, False}	True	True
Allow Phone	{True, False}	True	True
Common Policy Group			
Disable MMS	{True, False}	False	False
Disable Voice Note Recording	{True, False}	False	False
Security Policy Group			
Allow External Connections	{True, False}	True	True
Allow Internal Connections	{True, False}	True	True
Allow Third Party Apps to Use Serial Port	{True, False}	True	True
Content Protection Strength	0-2	Null	Null
Disable 3DES Transport Crypto	{True, False}	False	True*
Disable GPS	{True, False}	False	False
Disable External Memory	{True, False}	True	True
Disable USB Mass Storage	{True, False}	True	True
Disallow Third Party Application Downloads	{True, False}	False	False
Force Lock When Holstered	{True, False}	False	False
Device-Only Policy Group			
Allow Peer-to-Peer Messages	{True, False}	True	True
Allow SMS	{True, False}	True	True
Enable Long Term Timeout	{True, False}	False	False
Maximum Password Age	0-65535	0	0
Maximum Security Timeout	{1, 2, 5, 10, 15, 20, 30, 60}	60	60[8]
Minimum Password Length	4-14	4	4

[8] The allowed range of values for the Maximum Security Timeout IT policy is {2, 5, 10, 15, 20, 30, 60}. A value of 1 is not allowed in the evaluated configuration.

IT Policy Rule	Value		
	Range	Default	Baseline
Password Pattern Checks	0-3	0	1[9]
Password Required	{True, False}	False	True*
User Can Change Timeout	{True, False}	True	True
PIM Synch Policy Group			
Disable All Wireless Sync	{True, False}	False	False
Bluetooth Policy Group			
Disable Bluetooth	{True, False}	False	False
S/MIME Application Policy Group			
S/MIME Allowed Content Ciphers	0-7	ALL	{01,2 }[10]
Browser Policy Group			
Disable JavaScript in Browser	{True, False}	False	False
WLAN Policy Group			
Disable WLAN	{True, False}	False	False
Camera Policy Group			
Disable Camera	{True, False}	False	False
Disable Video Recorder	{True, False}	False	False
Password Policy Group			
Maximum Password History	0-15	0	0
Periodic Challenge Time	1-60	Null	Null
Set Maximum Password Attempts	3-10	10	10
Set Password Timeout	1-60	60	60
Suppress Password Echo	{True, False}	False	True*

8.2 Baseline Software Configuration

The baseline software configuration is the evaluated configuration of the TOE that provides the most flexibility to tailor the listed software configuration rules to comply with an enterprise security policy. The deployed configuration of the TOE shall be at least as restrictive as the baseline configuration. The following table identifies the valid range of values, default value, and baseline value for each software configuration rule specified in F.SWConfiguration. Modifying the baseline values will result in a more restrictive configuration, and thus may be configured to comply with an enterprise security policy while maintaining an evaluated configuration.

Table 13. Baseline Software Configuration

Software Configuration Rule	Value		
	Range	Default	Baseline
Disposition	{Optional, Required, Not Permitted}	Optional	Optional[11]

[9] The allowed range of values for the Password Pattern Checks IT policy rule is 1-3. A value of 0 is not allowed in the evaluated configuration.
[10] The allowed range of values for the S/MIME Allowed Content Ciphers IT policy rule is 0,1,2 . The values of 3, 4, 6, 7 are not allowed in the evaluated configuration.

Software Configuration Rule	Value		
	Range	Default	Baseline
Interprocess Communication	{Allowed, Not Permitted}	Allowed	Allowed
Internal Network Connections	{Prompt User, Allowed, Not Permitted}	Prompt User	Prompt User
External Network Connections	{Prompt User, Allowed, Not Permitted}	Prompt User	Prompt User
Local Connections	{Allowed, Not Permitted}	Allowed	Allowed
Phone Access	{Prompt User, Allowed, Not Permitted}	Prompt User	Prompt User
Message Access	{Allowed, Not Permitted}	Allowed	Allowed
PIM Data Access	{Allowed, Not Permitted}	Allowed	Allowed
Event Injection	{Allowed, Not Permitted}	Not Permitted	Not Permitted
Bluetooth Serial Profile	{Allowed, Not Permitted}	Allowed	Allowed
BlackBerry Device Keystore	{Allowed, Not Permitted}	Allowed	Allowed
BlackBerry Device Keystore Medium Security	{Allowed, Not Permitted}	Allowed	Allowed
Device GPS	{Prompt User, Allowed, Not Permitted}	Prompt User	Prompt User
User Authenticator API	{Allowed, Not Permitted}	Allowed	Allowed

8.3 Baseline User Guidance

In addition to the Smartphone being deployed on a BES with the Baseline (or stronger) policy, the Smartphone user must also ensure that under options / password that 'Allow calls while locked' is set to No. If it is set to yes, then contact information and a “place call” option on the menu of a locked device can be viewed. It should be noted that a previously paired Bluetooth headset or previously running application is expected to continue to function normally after a device has locked.

[11] Only applicable to trusted applications as defined by P.TrustedThirdParyApps in section 3.2.

9 Glossary

AES	Advanced Encryption Standard
API	Application Programming Interface
ANSI	American National Standards Institute
CBC	Cipher block chaining
CDMA	Code division multiple access
CLDC	Connected limited device configuration
EAL	Evaluation assurance level
ECDH	Elliptic curve Diffie-Hellman
ECDSA	Elliptic curve Digital Signature Algorithm
ECMQV	Elliptic curve Menezes, Qu, Vanstone
EDGE	Enhanced Data GSM Environment
EVDO	Evolution for Data Only
FIPS	Federal Information Processing Standard
GME	Gateway message envelope
GPRS	GSM general packet radio service
GPS	Global Positioning System
GSM	Global system for mobile communication
HMAC	Keyed-hashed message authentication code
iDEN	Integrated digital enhanced network
IEEE	Institute of Electrical and Electronics Engineers
IT	Information technology
MB	Megabytes
MIDP	Mobile information device profile
MMS	Multimedia Messaging Service
NV	Non-Volatile
PIM	Personal information management
PIN	Personal identification number
PRNG	Pseudo-random number generator
RAM	Random Access Memory
RIM	Research In Motion
RNG	Random number generator
SAR	Security assurance requirement
SFP	Security function policy
SFR	Security functional requirement
SHA	Secure Hash Algorithm
S/MIME	Secure/Multi-purpose Internet Mail Extensions
SMS	Short Messaging Service
SPP	Serial Port Profile
TOE	Target of evaluation

Triple DES	Triple Data Encryption Standard
TSC	TOE scope of control
TSF	TOE security functionality
UID	Unique identifier
USB	Universal Serial Bus
WAP	Wireless Application Protocol
WLAN	A type of local area network that uses high-frequency radio waves rather than wires to communicate between nodes.

*Check with service provider for availability, roaming arrangements and service plans. Certain features outlined in this document require a minimum version of BlackBerry Enterprise Server software, BlackBerry Desktop Software, and/or BlackBerry handheld software. May require additional application development. Prior to subscribing to or implementing any third party products or services, it is your responsibility to ensure that the airtime service provider you are working with has agreed to support all of the features of the third party products and services. Installation and use of third party products and services with RIM's products and services may require one or more patent, trademark or copyright licenses in order to avoid infringement of the intellectual property rights of others. You are solely responsible for determining whether such third party licenses are required and are responsible for acquiring any such licenses. To the extent that such intellectual property licenses may be required, RIM expressly recommends that you do not install or use these products and services until all such applicable licenses have been acquired by you or on your behalf. Your use of third party software shall be governed by and subject to you agreeing to the terms of separate software licenses, if any, for those products or services. Any third party products or services that are provided with RIM's products and services are provided "as is". RIM makes no representation, warranty or guarantee whatsoever in relation to the third party products and services and RIM assumes no liability whatsoever in relation to the third party products and services even if RIM has been advised of the possibility of such damages or can anticipate such damages.